Oracle® Fusion Middleware

Quick Installation Guide for Oracle Identity Management

11*g* Release 1 (11.1.1)

E10033-05

January 2011

Oracle Fusion Middleware Quick Installation Guide for Oracle Identity Management, 11*g* Release 1 (11.1.1)

E10033-05

Contents

3   Performing Common Installation Tasks

4   Installing and Configuring OID, OVD, ODSM, ODIP, and OIF (11.1.1.4.0)

5   Installing and Configuring OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0)

6   Configuring OIM Server, Design Console, and Remote Manager

Preface

This preface includes the following topics:

- Audience
- Documentation Accessibility
- Related Documents
- Conventions

Audience

This document is intended for users of Oracle Identity and Access Management.

Documentation Accessibility

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

Accessibility of Code Examples in Documentation

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

Accessibility of Links to External Web Sites in Documentation

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

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/support/contact.html or visit http://www.oracle.com/accessibility/support.html if you are hearing impaired.

Related Documents

For more information, see the following documents in the Oracle Fusion Middleware Release 11*g* Release 1 (11.1.1.3.0) documentation set:

- *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*
- *Oracle Fusion Middleware Administrator's Guide*

■ *Oracle Fusion Middleware Upgrade Guide for Oracle Identity Management*

Conventions

The following text conventions are used in this document:

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

1

Understanding Oracle Identity Management Installation

This chapter provides an overview of Oracle Identity Management 11*g* Release 1 (11.1.1) installation.

It includes the following topics:

- Overview and Structure of Oracle Identity Management 11g Installation
- Understanding OID, OVD, ODSM, ODIP, and OIF (11.1.1.4.0) Installation
- Understanding OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0) Installation

1.1 Overview and Structure of Oracle Identity Management 11*g* Installation

This section discusses the following topics:

- Overview
- Structure of the Installation

1.1.1 Overview

Oracle Identity Management 11*g* includes two distinct suites comprising the following Oracle Identity Management products:

- Oracle Identity Management 11g Release 1 (11.1.1.4.0) Components
- Oracle Identity Management 11g Release 1 (11.1.1.3.0) Components

Oracle Identity Management 11*g* Release 1 (11.1.1.4.0) Components

To install Oracle Identity Management 11*g* Release 1 (11.1.1.4.0) Components, you must install Oracle Identity Management 11*g* Release 1 (11.1.1.2.0) first.

To install Oracle Identity Management 11*g* Release 1 (11.1.1.2.0), use `ofm_idm_win_11.1.1.2.0_32_disk1_1of1.zip` (for **Windows**) or `ofm_idm_linux_11.1.1.2.0_32_disk1_1of1.zip` (for **Linux**) comprising the following products:

- Oracle Internet Directory (OID)
- Oracle Virtual Director (OVD)
- Oracle Directory Services Manager (ODSM)
- Oracle Directory Integration Platform (ODIP)
- Oracle Identity Federation (OIF)

Then you must patch your Oracle Identity Management 11.1.1.2.0 to Oracle Identity Management 11.1.1.4.0 using the `ofm_idm_win_11.1.1.4.0_32_disk1_1of1.zip` (for **Windows**) or `ofm_idm_linux_11.1.1.4.0_32_disk1_1of1.zip` (for **Linux**).

> **Note:** See Chapter 4, "Installing and Configuring OID, OVD, ODSM, ODIP, and OIF (11.1.1.4.0)" in this guide for installing and configuring these products.

Oracle Identity Management 11*g* Release 1 (11.1.1.3.0) Components

To install Oracle Identity Management 11*g* Release 1 (11.1.1.3.0) Components, use `ofm_iam_generic_11.1.1.3.0_disk1_1of1.zip` comprising the following Oracle Identity Management 11.1.1.3.0 products:

- Oracle Access Manager (OAM)

- Oracle Adaptive Access Manager (OAAM)

- Oracle Identity Manager (OIM)

- Oracle Authorization Policy Manager (OAPM)

- Oracle Identity Navigator (OIN)

> **Note:** See Chapter 5, "Installing and Configuring OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0)" in this guide for installing and configuring these products.

1.1.2 Structure of the Installation

You can install both of the Oracle Identity Management 11.1.1.3.0 (consisting of OIM, OAM, OAAM, OAPM, and OIN) and 11.1.1.4.0 (consisting of OID, OVD, ODSM, ODIP, and OIF) under a common Middleware Home directory. When you install these suites on the same machine, two Oracle Home (also referred to as IDM_ORACLE_HOME in this guide) directories are created on the machine. For information about identifying installation directories, see Identifying Installation Directories.

Note that two IDM_ORACLE_HOME directories are mentioned in descriptions and procedures throughout this guide. For example, the first one, **Oracle_IDM1** can be the IDM_Home directory for Oracle Internet Directory, Oracle Virtual Directory, Oracle Directory Services Manager, Oracle Directory Integration Platform, and Oracle Identity Federation. The second one, **Oracle_IDM2** can be the IDM_Home directory for Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Authorization Policy Manager, and Oracle Identity Navigator.

However, note that **Oracle_IDM1** and **Oracle_IDM2** are used as examples in this guide. You can specify any name for either of your IDM_Home directories. In addition, you can install the two distinct Oracle Identity Management suites in any order on your machine.

If you choose to use the default names, the first installation creates an **Oracle_IDM1** directory, and the second installation creates an **Oracle_IDM2** directory.

1.2 Understanding OID, OVD, ODSM, ODIP, and OIF (11.1.1.4.0) Installation

The following is an overview of the steps to install Oracle Internet Directory (OID), Oracle Virtual Directory (OVD), Oracle Directory Services Manager (ODSM), Oracle Directory Integration Platform (ODIP), and Oracle Identity Federation (OIF):

1. Review the certification information. For more information, see the following link:

   http://www.oracle.com/technetwork/middleware/ias/downloads/fusion-certification-100350.html

2. Review the system requirements. For more information, see the following link:

   http://www.oracle.com/technetwork/middleware/ias/downloads/fusion-requirements-100147.html

3. Satisfy all dependencies, such as installing Oracle WebLogic Server and, when required, installing an Oracle Database and creating schema.

4. Install the Oracle Identity Management 11.1.1.2.0 software, but do not configure the products.

5. Install Oracle Identity Management 11.1.1.4.0 software by running the Patch Set Installer to patch your existing Oracle Identity Management 11.1.1.2.0 software.

6. Run the Oracle Identity Management Configuration Wizard from the patched Oracle Identity Management Home directory to configure Oracle Internet Directory, Oracle Virtual Directory, Oracle Directory Services Manager, Oracle Directory Integration Platform, or Oracle Identity Federation.

7. Verify the installation.

1.3 Understanding OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0) Installation

The following is an overview of the steps to install Oracle Identity Manager (OIM), Oracle Access Manager (OAM), Oracle Adaptive Access Manager (OAAM), Oracle Authorization Policy Manager (OAPM), and Oracle Identity Navigator (OIN):

1. Review the certification information.

2. Review the system requirements.

3. Satisfy all dependencies, such as installing Oracle WebLogic Server and, when required, installing an Oracle Database and creating schemas.

4. Install the Oracle Identity Management 11.1.1.3.0 software containing Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Authorization Policy Manager, and Oracle Identity Navigator.

5. If you are installing Oracle Identity Manager, install the Oracle SOA Suite 11*g* Release 1 (11.1.1.2.0) software and patch it to Oracle SOA Suite 11*g* Release 1 (11.1.1.3.0) software by running the Patch Set Installer.

6. Run the Oracle Fusion Middleware Configuration Wizard to configure Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Authorization Policy Manager, or Oracle Identity Navigator.

7. If you are configuring Oracle Identity Manager, run the Oracle Identity Manager Configuration Wizard only once during the initial setup to configure Oracle Identity Manager Server, Design Console (on Windows only), and Remote

Manager. Note that you must run the Oracle Identity Manager Configuration Wizard on the machine where the WebLogic Administration Server is running.

8. Verify the installation.

2

Preparing to Install Oracle Identity Management

This chapter provides information you should review before installing Oracle Identity Management 11*g* Release 1 (11.1.1) components.

It includes the following topics:

- Before Installing OID, OVD, ODSM, ODIP, and OIF (11.1.1.4.0)
- Before Installing OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0)

Note: For information about prerequisites for installing the 11.1.1.2.0 version of Oracle Internet Directory (OID), Oracle Virtual Directory (OVD), Oracle Directory Services Manager (ODSM), Oracle Directory Integration Platform (ODIP), and Oracle Identity Federation (OIF) and patching them to 11.1.1.4.0, see Before Installing OID, OVD, ODSM, ODIP, and OIF (11.1.1.4.0).

For information about prerequisites for installing the 11*g* (11.1.1.3.0) version of Oracle Identity Manager (OIM), Oracle Access Manager (OAM), Oracle Adaptive Access Manager (OAAM), Oracle Authorization Policy Manager (OAPM), and Oracle Identity Navigator (OIN), see Before Installing OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0).

2.1 Before Installing OID, OVD, ODSM, ODIP, and OIF (11.1.1.4.0)

This topic provides information you should review before installing OID, OVD, ODSM, ODIP, and OIF (11.1.1.4.0).

This section discusses the following topics:

- System Requirements and Certification
- Installing and Configuring Java Access Bridge (Windows Only)
- Managing the Oracle WebLogic Server Node Manager Utility for Oracle Identity Management Installations
- Installing Oracle Database
- Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU)

2.1.1 System Requirements and Certification

Before performing any installation, read the system requirements and certification documentation to ensure that your environment meets the minimum installation requirements for the components you are installing. Both of these documents are available on Oracle Technology Network (OTN) web site at:

http://www.oracle.com/technetwork/middleware/ias/downloads/fusion-certification-100350.html

Oracle Fusion Middleware System Requirements, Prerequisites, and Specifications

The system requirements document covers information such as hardware and software requirements, minimum disk space and memory requirements, and required system libraries, packages, or patches:

http://www.oracle.com/technetwork/middleware/ias/downloads/fusion-requirements-100147.html

---

Note: The system requirements document also covers Oracle Universal Installer Startup Requirements.

Oracle Fusion Middleware Supported System Configurations

The certification document covers supported installation types, platforms, operating systems, databases, JDKs, and third-party products:

http://www.oracle.com/technetwork/middleware/ias/downloads/fusion-certification-100350.html

2.1.2 Installing and Configuring Java Access Bridge (Windows Only)

If you are installing Oracle Identity Management on a Windows 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 Web site:

   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.

2.1.3 Managing the Oracle WebLogic Server Node Manager Utility for Oracle Identity Management Installations

Oracle Directory Integration Platform (ODIP) and Oracle Identity Federation (OIF) are configured with a WebLogic domain. Oracle Internet Directory (OID) and Oracle Virtual Directory (OVD) can be configured with or without a WebLogic domain. For Oracle Identity Management products that require a WebLogic domain, you must configure Node Manager.

You must perform the following steps after installing Oracle WebLogic Server and before installing Oracle Identity Management:

1. Verify the Oracle WebLogic Server Node Manager utility is stopped. If it is running, kill the process. Use the following commands to identify running process and kill the same:

   For example, on UNIX:

   1) `ps-ef | grep -i nodemanager`

   This will return the Process Id of the Node Manager Process.

   2) `kill -9` <Process Id of the Node Manager Process>

   On Windows:

   Use the Windows Task Manager to identify running Node Manager processes and kill the same.

2. Determine if the `nodemanager.properties` file is present in the *WL_HOME*`/common/nodemanager/directory`.

   - If the nodemanager.properties file is *not* present, then follow the instructions below:

     On **UNIX**:

     Run `startNodeManager.sh` (Located at `<WL_HOME>/server/bin` directory) to start Node Manager.

     On **Windows**:

     Run `startNodeManager.cmd` (Located at `<WL_HOME>\server\bin` directory) to start Node Manager.

   - If the `nodemanager.properties` file *does* exist, open it and verify that the `ListenPort` parameter is included and that it is set. If the `ListenPort` parameter is not included or set, edit the nodemanager.properties file so that it is similar to the following, where *NODE_MANAGER_LISTEN_PORT* represents the port the Node Manager listens on, such as `5556`:

     `ListenPort=NODE_MANAGER_LISTEN_PORT`

2.1.4 Installing Oracle Database

You must install an Oracle Database before you can install some Oracle Identity Management components, such as:

- Oracle Internet Directory
- Oracle Identity Federation, if you want to use an RDBMS data store

For the latest information about supported databases, visit the following Web site:

http://www.oracle.com/technetwork/middleware/ias/downloads/fusion-certification-100350.html

The database must be up and running to install the relevant Oracle Identity Management component. The database does not have to be on the same system where you are installing the Oracle Identity Management component.

The database must also be compatible with Oracle Fusion Middleware Repository Creation Utility (RCU), which is used to create the schemas that Oracle Identity Management components require. For information about RCU requirements, refer to the system requirements document at the following Web site:

http://www.oracle.com/technetwork/middleware/ias/downloads/fusion-requirements-100147.html

2.1.5 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 Management components and configurations:

- Oracle Internet Directory, if you want to use an existing schema rather than create a new one using the Installer during installation.

Note: When you install Oracle Internet Directory, you have the choice of using an existing schema or creating a new one using the Installer. If you want to use an existing schema, you must create it using the Oracle Fusion Middleware Repository Creation Utility (RCU) before you can install Oracle Internet Directory. If you choose to create a new schema during installation, the Installer creates the appropriate schema for you and you do not need to use the RCU.

- Oracle Identity Federation Advanced configurations that use RDBMS for the Federation Store, Session Store, Message Store, or Configuration Store.

You create and load Oracle Fusion Middleware schema in your database using the RCU, which is available in the Oracle Fusion Middleware 11g Release 1 (11.1.1) release media and on the Oracle Technology Network (OTN) Web site. You can access the OTN web site at:

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

Note: RCU is available on Linux x86 and Windows x86 platforms only. Use the Linux RCU to create schemas on supported UNIX databases. Use Windows RCU to create schemas on supported Windows databases.

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

- For Oracle Internet Directory, select only the **Identity Management - Oracle Internet Directory** schema
- For Oracle Identity Federation, select only the **Identity Management - Oracle Identity Federation** schema

Note: When you create schema, be sure to remember the schema owner and password that is shown in RCU. For Oracle Identity Federation, it is of the form *PREFIX_OIF*. You will need to provide this information when configuring Oracle Identity Federation with RDBMS stores.

Do not change the prefix provided for Oracle Internet Directory.

See: The *Oracle Fusion Middleware Repository Creation Utility User's Guide* for complete information.

2.2 Before Installing OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0)

This section discusses the following topics:

- Oracle Fusion Middleware Certification
- System Requirements
- Installing and Configuring Java Access Bridge (Windows Only)
- Obtaining the Latest Oracle WebLogic Server and Oracle Fusion Middleware 11g Software
- Installing Oracle WebLogic Server 10.3.3 and Creating the Oracle Middleware Home
- Installing Oracle Database
- Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU)
- Upgrading an Existing Database Schema
- Installing the Latest Version of Oracle SOA Suite (Oracle Identity Manager Users Only)

2.2.1 Oracle Fusion Middleware Certification

The *Oracle Fusion Middleware Supported System Configurations* document provides certification information for Oracle Fusion Middleware, including supported installation types, platforms, operating systems, databases, JDKs, and third-party products related to Oracle Identity Management 11*g* Release 1 (11.1.1).

You can access the *Oracle Fusion Middleware Supported System Configurations* document by searching the Oracle Technology Network (OTN) web site:

```
http://www.oracle.com/technetwork/middleware/ias/downloads/fusio
n-certification-100350.html
```

2.2.2 System Requirements

This topic describes the system requirements for installing Oracle Identity Management 11*g* Release 1 (11.1.1) and includes the following sections:

- Most Recent Information
- Installer Startup Requirements
- Memory Requirements

2.2.2.1 Most Recent Information

The information in this topic is current at the time of publication. For the most recent information, refer to the *Oracle Fusion Middleware System Requirements, Prerequisites, and Specification* document, which contains information related to hardware, software, disk space, memory, system library, and patch requirements.

You can access the *Oracle Fusion Middleware System Requirements, Prerequisites, and Specification* document by searching the Oracle Technology Network (OTN) web site:

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

2.2.2.2 Installer Startup Requirements

When you start the Installer, it checks for the requirements listed in Table 2–1. The Installer will notify you if any requirements are not met.

Table 2–1   Installer Startup Requirements

Category	Minimum or Accepted Value
Platform	UNIX: ■ Solaris 9, Solaris 10 ■ HP-UX 11i (11.23), HP-UX 11i (11.31) ■ Oracle Enterprise Linux 4, Oracle Enterprise Linux 5, Red Hat Linux 4, Suse 11, Red Hat Linux 5, SUSE 10 ■ IBM AIX 5.3, IBM AIX 6.1 Windows: ■ Windows XP SP2 (Win32 platforms only), Windows 2003, Windows 2008, Windows Vista, Windows 7
CPU Speed	At least 300 MHZ
Temp Space	At least 500 MB
Swap Space	At least 500 MB
Monitor	At least 256 colors

2.2.2.3 Memory Requirements

Table 2–2 lists the minimum memory requirements to install Oracle Identity Management 11*g* Release 1 (11.1.1):

Table 2–2   Minimum Memory Requirements

Operating System	Minimum Physical Memory	Minimum Available Memory
Linux	2 GB	1 GB
UNIX	2 GB	1 GB
Microsoft Windows	2 GB	1 GB

The specific memory requirements for your Oracle Identity Management 11*g* Release 1 (11.1.1) deployment depends on which components, or combination of components, you install.

2.2.3 Installing and Configuring Java Access Bridge (Windows Only)

If you are installing Oracle Identity 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.

2.2.4 Obtaining the Latest Oracle WebLogic Server and Oracle Fusion Middleware 11*g* Software

Refer to the following for more information about the latest Oracle WebLogic Server and Oracle Fusion Middleware 11*g* software:

- You can download the latest Oracle Fusion Middleware 11*g* software from the Oracle Technology Network (OTN):

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

  For information about downloading Oracle WebLogic Server, see "Product Distribution" in the *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*.

- Oracle Fusion Middleware 11*g* also requires the latest version of Oracle WebLogic Server. At the time this document was published, the latest version of Oracle WebLogic Server was Oracle WebLogic Server 11*g* (10.3.3).

- For complete information about patching your Oracle Fusion Middleware 11*g* to the latest release, refer to the *Oracle Fusion Middleware Patching Guide*.

2.2.5 Installing Oracle WebLogic Server 10.3.3 and Creating the Oracle Middleware Home

Before you can install Oracle Identity Management 11*g* Release 1 (11.1.1) components, you must install Oracle WebLogic Server and create the Oracle Middleware Home directory.

Complete the following steps to install Oracle WebLogic Server and create the Oracle Middleware Home directory. You can refer to the *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server* for complete information about installing Oracle WebLogic Server.

1. Insert the Oracle WebLogic Server CD-ROM or download the Oracle WebLogic Server Installer from the following URL:

http://www.oracle.com/technetwork/middleware/weblogic/downloads/index.html

For information about downloading Oracle WebLogic Server, see "Product Distribution" in the *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*.

2. Locate the appropriate executable file for your system, such as:

- `wls_linux32.bin` for 32-bit Linux systems
- `wls_win32.exe` for 32-bit Windows systems
- `wls_generic.jar` for all 64-bit platforms

The 32-bit executable files are bundled with the appropriate JDK version. If you use the 64-bit installer, you will need to invoke the installer with a supported JDK for your platform. This JDK must be installed on your system before you install Oracle WebLogic Server. Refer to the Oracle Fusion Middleware certification document for a list of supported JDKs for your platform:

http://www.oracle.com/technetwork/middleware/ias/downloads/fusion-certification-100350.html

3. Run the Oracle WebLogic Server Installer directly from the CD-ROM, or copy the file to your local system and run it locally.

For example, on 32-bit systems:

Linux:

```
./wls_linux32.bin
```

Windows:

```
wls_win32.exe
```

For example, on 64-bit systems:

UNIX:

```
JAVA_HOME/bin/java -jar wls_generic.jar
```

or

```
JAVA_HOME/bin/java -d64 -jar wls_generic.jar
```

Windows:

```
JAVA_HOME\bin\java -jar wls_generic.jar
```

For 64-bit installations:

- Before running the installer, set the `DISPLAY` environment variable on your system (for **UNIX** only).

- Replace *JAVA_HOME* with the installation location of the supported JDK you installed for your platform.

- Use the `-d64` flag when using 32/64-bit hybrid JDKs (such as the HP JDK for HP-UX and SUN JDK for Solaris SPARC).

- Execute *JAVA_HOME*`/bin/java -version` (or *JAVA_HOME*`/bin/java -d64 -version` on 32/64-bit hybrid JDKs) to ensure that your *JAVA_HOME* refers to a 64-bit JDK.

Note: After you start the Oracle WebLogic Server Installer, the Welcome screen appears.

---

4. Click **Next**. The Choose Middleware Home Directory screen appears.

5. Select **Create a new Middleware Home** and identify the desired location for your new Middleware Home directory, which is the top-level directory for all Oracle Fusion Middleware products. The WebLogic Home directory will be created inside the Middleware Home directory.

Note: If the Middleware Home directory already exists on your system, it must be an empty directory. Do not enter any special characters in the name of the Middleware Home directory.

Click **Next**. The Register for Security Updates screen appears.

6. Select whether or not you want to receive the latest product and security updates. If you choose not to receive anything, you will be asked to verify your selection before continuing.

   Click **Next**. The Choose Install Type screen appears.

7. Select the **Typical** install type and click **Next**. The JDK Selection screen appears. On this screen, select the Sun JDK or the Oracle JRockit JDK. Click **Next**.

   The Choose Product Installation Directories screen appears.

8. Specify the desired location for your WebLogic Server Home directory and click **Next**.

   If you are installing Oracle WebLogic Server on a UNIX system, the Installation Summary screen appears. Go to step 9 now.

   If you are installing Oracle WebLogic Server on a Windows system, the Choose Shortcut Location screen appears. Specify a location where you want Windows to create a shortcut to Oracle products and click **Next**. The Installation Summary screen appears.

9. Click **Next** on the Installation Summary screen.

   The Installation Progress screen appears.

10. Click **Next**. The Installation Complete screen appears.

11. De-select **Run Quickstart** and click **Done** to exit the Installer.

   Notes:

   - The same user that installed Oracle WebLogic Server must install Oracle Identity Management.

   - Do not log in to the Oracle WebLogic Server Administration Console during Oracle Identity Management installation.

Oracle WebLogic Server Directory Structure

After you install Oracle WebLogic Server and create a Middleware Home, a home directory, such as `wlserver_10.3`, is created for Oracle WebLogic Server under your Middleware Home. This home directory is referred to as WL_HOME.

At the same level as WL_HOME, separate directories are created for the following components associated with Oracle WebLogic Server:

- Sun JDK - `jdk160_18`

- Oracle JRockit - `jrockit_160_17_R28.0.0-679`

Note that 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 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.

2.2.6 Installing Oracle Database

You must install an Oracle Database before you can install some Oracle Identity Management components. The database must be up and running to install the relevant

Oracle Identity Management component. The database does not have to be on the same system where you are installing the Oracle Identity Management component.

The following database versions are supported:

- 10.2.0.4
- 11.1.0.7
- 11.2

> **Note:** You can locate the most recent information about supported databases by referring to the "Oracle Fusion Middleware Certification" topic in this chapter.

Table 2–3 lists the databases requirements for RCU at the time of publication:

Table 2–3   RCU Database Requirements

Category	Minimum or Accepted Value
Version	Oracle Database 10.2.0.4, 11.1.0.7, or 11.2 (11.1.0.7 or later for non-XE database). **Note**: When installing the database, you must choose the AL32UTF8 character set.
Shared Pool Size	147456 KB
SGA Maximum Size	147456 KB
Block Size	8 KB
Processes	500

> **Note:** If you are using Oracle Database 11.1.0.7 for Oracle Identity Manager, you should install a set of platform-specific patches before creating Oracle Identity Manager schemas. For more information, see the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.
>
> After installing the Oracle 11*g* database, you must complete the following steps:
>
> 1. Log in to the database as the `sys` (default) user.
> 2. Run the following commands:
>
>    ```
>    alter system set session_cached_cursors=100
>    scope=spfile;
>
>    alter system set processes=500 scope=spfile;
>    ```
>
> 3. Bounce the database and continue with the installation of Oracle Fusion Middleware Repository Creation Utility (RCU) and loading of schemas.

2.2.7 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 Management components and configurations:

- Oracle Identity Manager
- Oracle Access Manager

- Oracle Adaptive Access Manager

- Oracle Authorization Policy Manager

You create and load Oracle Fusion Middleware schema in your database using the Oracle Fusion Middleware Repository Creation Utility (RCU), which is available in the Oracle Fusion Middleware 11*g* Release 1 (11.1.1) release media and on the Oracle Technology Network (OTN) web site. You can access the OTN web site at:

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

> **Note:** RCU is available only on Linux and Windows platforms. Use the Linux RCU to create schemas on supported UNIX databases. Use Windows RCU to create schemas on supported Windows databases. After you extract the contents of the rcuHome.zip file to a directory, you can see the executable file rcu in the BIN directory.
>
> 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 about troubleshooting RCU, see the "Troubleshooting Repository Creation Utility" topic in the guide *Oracle Fusion Middleware Repository Creation Utility User's Guide*.

When you run RCU, create and load only the following schema for the Oracle Identity 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 the "OAAM Partition Schema Reference" topic in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

- 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 Authorization Policy Manager, select the **Identity Management - Authorization Policy Manager** 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.

> **See:** The *Oracle Fusion Middleware Repository Creation Utility User's Guide* for complete information.

2.2.8 Upgrading an Existing Database Schema

If you want to reuse an existing database schema, you must upgrade your old database schema to work with Oracle Fusion Middleware 11g products and components.

For information about upgrading your existing database schema, see *Oracle Fusion Middleware Upgrade Guide for Oracle Identity Management*.

2.2.9 Installing the Latest Version of Oracle SOA Suite (Oracle Identity Manager Users Only)

If you are installing Oracle Identity Manager, you must install the latest version of Oracle SOA Suite (11.1.1.3.0).

Follow the instructions in this section to install the latest Oracle SOA Suite software. The installation of Oracle SOA Suite is a prerequisite for configuring Oracle Identity Manager.

Installing the latest version of Oracle SOA Suite 11*g* involves the following steps:

1. Obtaining the Latest Oracle WebLogic Server and Oracle SOA Suite Software

2. Installing Oracle WebLogic Server and Creating the Middleware Home

3. Installing the Latest Version of Oracle SOA Suite

4. Patching the Software to 11.1.1.3.0

2.2.9.1 Obtaining the Latest Oracle WebLogic Server and Oracle SOA Suite Software

Refer to the following for more information about the latest Oracle WebLogic Server and Oracle Fusion Middleware 11*g* software:

- You can download the latest Oracle Fusion Middleware 11*g* software from the Oracle Technology Network (OTN):

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

- At the time this document was published, the latest release of Oracle Fusion Middleware 11*g* was 11*g* Release 1 (11.1.1.3.0), which provides new features and capabilities that supersede those available in Oracle Fusion Middleware 11*g* Release 1 (11.1.1.1.0) and 11*g* Release 1 (11.1.1.2.0).

- Oracle Fusion Middleware 11*g* also requires the latest version of Oracle WebLogic Server. At the time this document was published, the latest version of Oracle WebLogic Server was Oracle WebLogic Server 11*g* Release 1 (10.3.3).

- For complete information about patching your Oracle Fusion Middleware 11*g* to the latest release, refer to the *Oracle Fusion Middleware Patching Guide*.

2.2.9.2 Installing Oracle WebLogic Server and Creating the Middleware Home

Oracle SOA Suite requires Oracle WebLogic Server and a Middleware Home directory. For more information, see "Install Oracle WebLogic Server" in *Oracle Fusion Middleware Installation Planning Guide*. In addition, see "Running the Installation Program in Graphical Mode" in *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*.

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

2.2.9.3 Installing the Latest Version of Oracle SOA Suite

Note that only Oracle Identity Manager requires Oracle SOA Suite 11*g* (11.1.1.3.0). This step is required because Oracle Identity Manager uses process workflows in Oracle SOA Suite to manage request approvals.

Follow the instructions in Table 2–4 to install Oracle SOA Suite. If you need additional help with any of the installation screens, click **Help** to access the online help.

To start the Oracle SOA Suite installation wizard, you must complete the following steps:

1. Extract the contents of the `soa.zip` (11.1.1.2.0) to a directory, such as `soa`.

2. From your present working directory, move to the `Disk1` directory under `soa`.

3. From the `Disk1` directory, run `runInstaller` (on UNIX) or `setup.exe` (on Windows) executable files to launch the Oracle SOA Suite 11.1.1.2.0 installation wizard.

Table 2–4   Installation Flow for Install Only Option

No.	Screen	Description and Action Required
1	Welcome Screen	Click **Next** to continue.
2	Prerequisite Checks Screen	Click **Next** to continue.
3	Specify Installation Location Screen	Specify the Middleware Home and Oracle Home locations. You must specify the location of the same Middleware Home that contains Oracle Identity Management components.
		For more information about these directories, see "Oracle Fusion Middleware Directory Structure and Concepts" in *Oracle Fusion Middleware Installation Planning Guide*.
		Click **Next** to continue.
4	Specify Security Updates Screen	Provide your E-mail address to be informed of the latest product issues.
		Click **Next** to continue.

Table 2–4   (Cont.) Installation Flow for Install Only Option

No.	Screen	Description and Action Required
5	Installation Summary Screen	Verify the information on this screen. Click **Install** to begin the installation.
6	Installation Progress Screen	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. Click **Next** to continue.
7	Installation Complete Screen	Click **Finish** to dismiss the installer.

> **Note:**   At this stage of the installation process, do not configure a WebLogic domain for Oracle SOA Suite.

2.2.9.4 Patching the Software to 11.1.1.3.0

After the installation is complete, you must run the Patch Set Installer for Oracle SOA Suite (included in the Disk1 directory under the soa_patchset.zip file) to update your 11.1.1.2.0 software to the latest version of Oracle SOA Suite (11.1.1.3.0).

For instructions, go to "Applying the Latest Oracle Fusion Middleware Patch Set with the Patch Set Installers" in *Oracle Fusion Middleware Patching Guide*.

3

Performing Common Installation Tasks

This chapter describes tasks that are common to most Oracle Identity Management installations and configurations. It includes the following topics:

- Common Installation Tasks for OID, OVD, ODSM, ODIP, and OIF (11.1.1.4.0)

- Common Installation Tasks for OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0)

Note: By completing the common installation tasks described in this chapter, you are not installing or configuring the Oracle Identity Management software.

For complete information about installing and configuring Oracle Identity Management software, see the following links:

- Installing and Configuring OID, OVD, ODSM, ODIP, and OIF (11.1.1.4.0)

- Installing and Configuring OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0)

3.1 Common Installation Tasks for OID, OVD, ODSM, ODIP, and OIF (11.1.1.4.0)

This section discusses the following topics:

- Starting an Installation

- Creating the Inventory Directory (UNIX Only)

- Identifying Installation Directories

- Determining Port Numbers

- Completing an Installation

- Optional: Configuring the Minimum Amount for Oracle WebLogic Server's Maximum Heap Size

- Locating Installation Log Files

3.1.1 Starting an Installation

This topic explains the steps that are common to starting most Oracle Identity Management installations and configurations. It begins with starting the Installer and ends after you complete the steps on the Prerequisites Check screen.

> **Note:** You must be logged in to the UNIX operating system as a
> non-root user to start the Installer.
>
> This command to start the installation program applies to the
> following Oracle Identity Management Installers:
>
> ■ Oracle Identity Management 11*g* Release 1 (11.1.1.2.0).
>
> ■ Oracle Identity Management 11*g* Release 1 (11.1.1.4.0) patchset
> Installer.

Perform the following steps to start an Oracle Identity Management installation:

1. Start the Installer by executing one of the following commands:

   UNIX: `./runInstaller`

   Windows: *DRIVE*`:\setup.exe`

   After the Installer starts, the Welcome screen appears.

2. Continue the installation or patching process by clicking **Next** on the Welcome
   screen.

   For more information about patching an Oracle Identity Management 11.1.1.2.0
   installation to 11.1.1.4.0, see Patching the Oracle Identity Management 11.1.1.2.0 to
   11.1.1.4.0

3.1.2 Creating the Inventory Directory (UNIX Only)

If you are installing on a UNIX system, and if this is the first time any Oracle product
is being installed on your system with the Oracle Universal Installer, you will be asked
to provide the location of an inventory directory. This is where the installer will set up
subdirectories and maintain inventory data for each Oracle product that is installed on
this system.

Follow the instructions in Table 3–1 to configure the inventory directory information:

Table 3–1   Inventory Directory and Group Screens

Screen	Description
Specify Inventory Directory	Specify the Oracle inventory directory and group permissions for that directory. The group must have write permissions to the Oracle inventory directory.
	Click **OK** to continue.
Inventory Location Confirmation	Run the createCentralInventory.sh script as root.
	Click **OK** to continue.

> **Note:** If you do not want to use the central inventory, you can create
> the oraInst.loc file, add the custom location of the inventory, and run
> the runInstaller by using the following command:
>
> `runInstaller -invPtrLoc <full location to`
> `oraInst.loc>`

3.1.3 Identifying Installation Directories

This topic describes directories you must identify in most Oracle Identity 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
- WebLogic Server Directory
- Oracle Instance Location
- Oracle Instance Name

3.1.3.1 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 Installer also creates an Oracle Common Home directory under the Oracle Middleware Home. The Oracle Common Home contains the binary and library files required for Oracle Enterprise Manager Fusion Middleware Control and Oracle Java Required Files (JRF). There can be only one Oracle Common Home within each Oracle Middleware Home.

The Oracle Middleware Home directory is commonly referred to as *MW_HOME*.

> **Note:** To install Oracle Identity Management components in an existing Oracle WebLogic Server administration domain, each Oracle Middleware Home directory in the domain must have identical directory paths and names.

3.1.3.2 Oracle Home Directory

Enter a name for the component's Oracle Home directory. 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 (such as binaries and libraries) required to host the component in the Oracle Home directory.

The Oracle Home directory is commonly referred to as *ORACLE_HOME*.

> **Note:** To install Oracle Identity Management components in an existing Oracle WebLogic Server administration domain, each Oracle Home directory in the domain must have identical directory paths and names.

3.1.3.3 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*.

> **Note:** To install Oracle Identity Management components in an existing Oracle WebLogic Server administration domain, each Oracle WebLogic Server Home directory in the domain must have identical directory paths and names.

3.1.3.4 Oracle Instance Location

Enter the path to the location where you want to create the Oracle Instance directory. The Installer creates the Oracle Instance directory using the location you enter in this field and using the name you enter in the Oracle Instance Name field. Do not enter a path to an existing directory that contains files—if you enter a path to an existing directory, that directory must be empty.

The Installer installs the component's configuration files in the Oracle Instance directory. Runtime components will write only to this directory. You can identify any location on your system for the Oracle Instance directory—it does not have to reside inside the Oracle Middleware Home directory.

3.1.3.5 Oracle Instance Name

Enter a name for the Oracle Instance directory. The Installer uses the name you enter in this field to create the Oracle Instance directory at the location you specify in the Oracle Instance Location field. This directory is commonly referred to as *ORACLE_INSTANCE*.

Instance names are important because Oracle Fusion Middleware uses them to uniquely identify instances. If you install multiple Oracle Fusion Middleware instances on the same computer, for example, an Oracle Identity Management instance and an Oracle WebLogic Server instance, you must give them different names.

The name you enter for the Oracle Instance directory must:

- Contain only alphanumeric and underscore (_) characters
- Begin with an alphabetic character (a-z or A-Z)
- Consist of 4-30 characters
- Not contain the hostname or IP address of the computer

> **Note:** You cannot change the Oracle Instance name after installation.

3.1.4 Determining Port Numbers

If you want to install an Oracle Identity Management 11*g* Release 1 (11.1.1) component against an existing Oracle Identity 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 Directory Integration Platform 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 Directory Integration Platform.

You can get information about ports using the following:

- WebLogic Server Administration Console.

  Log in to the Administration Console. Click on **Servers** under **Environment** to see what ports are in use for the Administration Server and Managed Servers.

> **Note:** For Oracle Internet Directory, you cannot get information about ports using WebLogic Server Administration Console.

- `$ORACLE_INSTANCE/config/OPMN/opmn/ports.prop`

  > **Note:** If you change a component's port number after installation, the ports.prop file is *not* updated.

- The `$ORACLE_INSTANCE/bin/opmnctl` status -l command to see port numbers of components managed by Oracle Process Manager and Notification Server (OPMN).

3.1.5 Completing an Installation

This topic explains the steps that are common to completing most Oracle Identity Management installations and configurations. It begins with the steps on the Installation Summary screen and ends after the Installation Complete screen.

When the Installation Summary screen appears, perform the following steps to complete the installation:

1. Verify the installation and configuration information on the Installation Summary screen.

   - Click **Save** to save the installation response file, which contains your responses to the Installer prompts and fields. You can use this response file to perform silent installations.

     > **Note:** The installation response file is not saved by default—you must click **Save** to retain it.

   - Click **Install**. The Installation Progress screen appears.

2. Monitor the progress of your installation. The location of the installation log file is listed for reference. After the installation progress reaches 100%, the Configuration Progress screen appears.

   > **Note:** On UNIX systems, after the installation progress reaches 100%, a confirmation dialog box appears with information about the oracleRoot.sh script. Execute the script in different terminal and continue to the Configuration Progress screen. For more information, see the "Executing the oracleRoot.sh Script on UNIX Platforms" topic in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

3. Monitor the progress of the configuration. The location of the configuration log file is listed for reference. After the configuration progress reaches 100%, the Installation Complete screen appears.

4. By default the installation summary file, which can help you get started with administration, is saved to the *OUI_INVENTORY*/logs/ directory. The filename is of the form: installSummary*DATE*.txt. This file contains information about the

configuration, such as locations of install directories and URLs for management components.

If desired, you can click the **Save** button on the Installation Complete screen and choose a different name and location for the file.

Click **Finish** to close and exit the Installer.

3.1.6 Optional: Configuring the Minimum Amount for Oracle WebLogic Server's Maximum Heap Size

After installing Oracle Identity Management 11*g* Release 1 (11.1.1), if you want to configure the minimum (lowest) level of maximum heap size (-Xmx) required for Oracle WebLogic Server to host Oracle Identity Management components, perform the steps in this section.

> **Note:** This is an *optional* step, typically performed only for test, development, or demonstration environments.
>
> This procedure applies to OID, OVD, ODSM, ODIP, and OIF only.

The minimum (lowest) levels for maximum heap size are:

- Oracle WebLogic Administration Server: 512 MB
- Oracle WebLogic Managed Server: 256 MB

Perform the following steps to configure the heap size for Oracle WebLogic Administration Servers and Oracle WebLogic Managed Servers:

1. Open the setDomainEnv script (.sh or .bat) in the *MW_HOME*/user_projects/domains/*DOMAIN_NAME*/bin/ directory.

2. Locate the *last* occurrence of the EXTRA_JAVA_PROPERTIES entry.

3. In the last occurrence of the EXTRA_JAVA_PROPERTIES entry, locate the *last* occurrence of heap size parameters: -Xmx, -Xms, and so on.

    > **Note:** These are the heap size parameters for the Oracle WebLogic Administration Server.

4. Set the heap size parameters (-Xms and -Xmx) for the Oracle WebLogic Administration Server as desired, for example: -Xms256m and -Xmx512m

5. To set the heap size parameters for the Oracle WebLogic Managed Server, enter the text in Example 3–1 immediately below the *last* occurrence of the EXTRA_JAVA_PROPERTIES entry and:

    - Set the heap size parameters (-Xms and -Xmx) as desired, for example: -Xms256m -Xmx256m

    - Replace wls_ods1 with the name of the Oracle WebLogic Managed Server hosting Oracle Directory Services Manager.

    - Replace wls_oif1 with the name the Oracle WebLogic Managed Server hosting Oracle Identity Federation.

Example 3–1   Heap Size Parameters for Oracle WebLogic Managed Server

```
if [ "${SERVER_NAME}" = "wls_ods1" -o  "${SERVER_NAME}" = "wls_oif1" ] ; then
        EXTRA_JAVA_PROPERTIES=" ${EXTRA_JAVA_PROPERTIES} -Xms256m -Xmx256m "
        export EXTRA_JAVA_PROPERTIES
fi
```

6. Save and close the `setDomainEnv` script.

7. Restart the Oracle WebLogic Administration Server and the Oracle WebLogic Managed Server by referring to Starting the Stack.

> **Note:** On UNIX systems, if you execute the `ps -ef` command and `grep` for `AdminServer` or the name of the Oracle WebLogic Managed Server (for example, `ps -ef | grep AdminServer` or `ps -ef | grep wls_oif1`), the output contains multiple occurrences of heap size parameters (-Xmx and -Xms).
>
> Be aware that the last occurrence of the heap size parameters in the output are effective and have precedence over the preceding occurrences.

3.1.7 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

3.2 Common Installation Tasks for OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0)

This section discusses the following topics:

- Starting an Installation
- Starting Oracle Fusion Middleware Configuration Wizard
- List of Executable Files
- Identifying Installation Directories

- Determining Port Numbers
- Completing an Installation
- Locating Installation Log Files

3.2.1 Starting an Installation

This topic explains the steps that are common to starting most Oracle Identity Management installations and configurations. It begins with starting the Installer and ends after you complete the steps on the Prerequisites Check screen.

> **Note:** Starting the Installer as the `root` user is not supported.

Perform the following steps to start an Oracle Identity Management installation:

1. Extract the contents of the `iamsuite.zip` file to a directory. By default, this directory is named `iamsuite`.

2. Move to the `Disk1` directory under the `iamsuite` folder.

3. Start the Installer by executing one of the following commands:

   UNIX: `<full path to the runInstaller directory>/runInstaller -jreLoc <Middleware Home>/jrockit_160_05_R27.6.2-20/jre`

   Windows: `<full path to the setup.exe directory>\ setup.exe -jreLoc <Middleware Home>\jrockit_160_05_R27.6.2-20\jre`

   > **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 `jrockit_160_05_R27.6.2-20` 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 `D:\oracle\Middleware\jrockit_160_05_R27.6.2-20`, then launch the installer from the command prompt as follows:
   >
   > `D:\setup.exe -jreLoc D:\oracle\Middleware\jrockit_ 160_05_R27.6.2-20\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.

After the Installer starts, the Welcome screen appears. Continue by referring to the appropriate procedure in this document for the installation you want to perform.

3.2.2 Starting Oracle Fusion Middleware Configuration Wizard

To start the Oracle Fusion Middleware Configuration Wizard, which is used to configure Oracle Identity Management products in a new or existing WebLogic

administration domain, run the `<IDM_Home>/common/bin/config.sh` script (on UNIX). On Windows, run the `<IDM_Home>\common\bin\config.bat` script. The Oracle Fusion Middleware Configuration Wizard is displayed.

> **Note:** When you run the `config.cmd` or `config.sh` command, the following error message might be displayed:
>
> `*sys-package-mgr*: can't create package cache dir`
>
> The error message indicates that the default cache directory is not valid. You can change the cache directory by including the `-Dpython.cachedir=<valid_directory>` option in the command line.

3.2.3 List of Executable Files

Table 3–2 lists the executable files that are included in the Oracle WebLogic Server, Oracle Identity Management, Oracle SOA Suite, Oracle Web Tier, and Oracle HTTP Server 11*g* WebGate for Oracle Access Manager Installers.

Table 3–2   Executable Files

Name of the File	Description
`iamsuite.zip`	Oracle Identity Management 11*g* Release 1 (11.1.1) Installer for Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Authorization Policy Manager, and Oracle Identity Navigator
`wls_linux32.bin` for 32-bit Linux systems, `wls_win32.exe` for 32-bit Windows systems, and `wls_generic.jar` for all 64-bit platforms	Oracle WebLogic Server 10.3.3 Installer
`soa.zip`	Oracle SOA Suite 11*g* (11.1.1.2.0) Installer
`soa_patchset.zip`	Oracle SOA Suite 11*g* (11.1.1.3.0) Patch Set Installer
`webtier.zip`	Oracle Web Tier 11*g* (11.1.1.2.0) Installer
`webgate.zip`	Oracle HTTP Server 11*g* WebGate for Oracle Access Manager Installer
`rcuHome.zip`	Oracle Fusion Middleware Repository Creation Utility

3.2.4 Identifying Installation Directories

This topic describes directories you must identify in most Oracle Identity 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

3.2.4.1 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*.

3.2.4.2 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.

3.2.4.3 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*.

3.2.4.4 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)*.

3.2.4.5 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*.

3.2.5 Determining Port Numbers

If you want to install an Oracle Identity Management 11*g* Release 1 (11.1.1) component against an existing Oracle Identity 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.

3.2.6 Completing an Installation

This topic explains the steps that are common to completing most Oracle Identity Management installations and configurations. It begins with the steps on the Installation Summary screen and ends after the Installation Complete screen.

When the Installation Summary screen appears, perform the following steps to complete the installation:

1. Verify the installation and configuration information on the Installation Summary screen.

   - Click **Save** to save the installation response file, which contains your responses to the Installer prompts and fields. You can use this response file to perform silent installations. Refer to the topic "Performing Silent Installations" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

     > **Note:** The installation response file is not saved by default—you must click **Save** to retain it.

   - Click **Install**. The Installation Progress screen appears.

2. Monitor the progress of your installation. The location of the installation log file is listed for reference. After the installation progress reaches 100%, click **OK**. The Installation Complete screen appears.

3. Click **Save** to save the installation summary file. This file contains information about the configuration, such as locations of install directories, that will help you get started with configuration and administration.

     > **Note:** The installation summary file is not saved, by default—you must click **Save** to retain it.

   Click **Finish** to close and exit the Installer.

3.2.7 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

4

Installing and Configuring OID, OVD, ODSM, ODIP, and OIF (11.1.1.4.0)

This chapter describes how to install and configure OID, OVD, ODSM, ODIP, and OIF (11.1.1.4.0).

This chapter includes the following topics:

- Installing and Configuring OID, OVD, ODSM, ODIP, and OIF (11.1.1.4.0)
- OID with ODIP, ODSM, and Fusion Middleware Control in a New WebLogic Domain
- Only OID Without a WebLogic Domain
- OVD with ODSM and Fusion Middleware Control in a New WebLogic Domain
- OIF with OID in a New WebLogic Domain for LDAP Authentication, User Store, and Federation Store

4.1 Installing and Configuring OID, OVD, ODSM, ODIP, and OIF (11.1.1.4.0)

Follow the instructions in this section to install and configure the latest version of Oracle Internet Directory (OID), Oracle Virtual Directory (OVD), Oracle Directory Services Manager (ODSM), Oracle Directory Integration Platform, and Oracle Identity Federation (OIF).

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

1. Obtaining Oracle Fusion Middleware 11g Software

2. Installing Oracle WebLogic Server 11g (10.3.4) and Creating the Middleware Home

3. Installing the 11.1.1.2.0 Version of Oracle Identity Management Software

4. Patching the Oracle Identity Management 11.1.1.2.0 to 11.1.1.4.0

5. Configuring Your Components

> **Note:** If you have an existing Oracle Identity Management installation refer to *Oracle Fusion Middleware Patching Guide* or Oracle Fusion Middleware Upgrade Guide for Oracle Identity Management.

4.1.1 Obtaining Oracle Fusion Middleware 11*g* Software

■ You can download the latest Oracle Fusion Middleware 11*g* software from the Oracle Technology Network (OTN):

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

You must ensure that you have the following versions of Oracle Fusion Middleware Software:

– Oracle WebLogic Server 11g (10.3.4)

– Oracle Identity Management 11*g* Release 1 (11.1.1.2.0)

– Oracle Identity Management 11*g* Release 1 (11.1.1.4.0)

> **Note:** If you have not installed Oracle Identity Management 11.1.1.2.0 on your machine, you must download both 11.1.1.2.0 and 11.1.1.4.0 versions of the software. You must install the 11.1.1.2.0 version by choosing the **Install Software - Do Not Configure** option. Then you must patch the 11.1.1.2.0 software by running the 11.1.1.4.0 Patch Set Installer.

For information about downloading Oracle WebLogic Server, see "Product Distribution" in the *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*.

■ Oracle Fusion Middleware 11*g* also requires the latest version of Oracle WebLogic Server. At the time this document was published, the latest version of Oracle WebLogic Server was Oracle WebLogic Server 11*g* (10.3.4).

■ For complete information about patching your Oracle Fusion Middleware 11*g* to the latest release, refer to the *Oracle Fusion Middleware Patching Guide*.

4.1.2 Installing Oracle WebLogic Server 11*g* (10.3.4) and Creating the Middleware Home

Oracle Identity Management requires Oracle WebLogic Server and a Middleware home directory.

For more information, see "Install Oracle WebLogic Server" in *Oracle Fusion Middleware Installation Planning Guide*. In addition, see "Running the Installation Program in Graphical Mode" in *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*.

> **Note:** If you are installing Oracle Internet Directory 11g Release 1 (11.1.1.4.0) without an Oracle WebLogic administration domain, you do not need to install Oracle WebLogic.

Perform the following steps to install Oracle WebLogic Server and create the Oracle Middleware Home directory. You can refer to the *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server* for complete information about installing Oracle WebLogic Server.

1. Insert the Oracle WebLogic Server CD-ROM or download the Oracle WebLogic Server Installer from the following Web site:

http://www.oracle.com/technetwork/middleware/weblogic/downloads/index.html

2. Locate the appropriate executable file for your system, such as:

- wls1034_linux32.bin for 32-bit Linux systems
- wls1034_win32.exe for 32-bit Windows systems
- wls1034_generic.jar for all 64-bit platforms

The 32-bit executable files are bundled with the appropriate JDK version. If you use the 64-bit installer, you will need to invoke the installer with a supported JDK for your platform. This JDK must be installed on your system before you install Oracle WebLogic Server. Refer to the Oracle Fusion Middleware certification document for a list of supported JDKs for your platform:

http://www.oracle.com/technetwork/middleware/ias/downloads/fusion-certification-100350.html

For more information about downloading Oracle WebLogic Server, see "Product Distribution" in the *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*.

3. Run the Oracle WebLogic Server Installer directly from the CD-ROM, or copy the file to your local system and run it locally. For 64-bit installations:

- Before running the installer, set the `DISPLAY` environment variable on your system.
- Replace *JAVA_HOME* with the installation location of the supported JDK you installed for your platform.
- Use the `-d64` flag when using 32/64-bit hybrid JDKs (such as the HP JDK for HP-UX and SUN JDK for Solaris SPARC).
- Execute *JAVA_HOME*`/bin/java -version` (or *JAVA_HOME*`/bin/java -d64 -version` on 32/64-bit hybrid JDKs) to ensure that your *JAVA_HOME* refers to a 64-bit JDK.

Examples for 32-bit systems:

Linux:

```
./wls1034_linux32.bin
```

Windows:

```
wls1034_win32.exe
```

Examples for 64-bit systems:

UNIX:

```
JAVA_HOME/bin/java -jar wls1034_generic.jar
```

or

```
JAVA_HOME/bin/java -d64 -jar wls1034_generic.jar
```

Windows:

```
JAVA_HOME\bin\java -jar wls1034_generic.jar
```

> **Note:** After you start the Oracle WebLogic Server Installer, the Welcome screen appears.

4. Click **Next**. The Choose Middleware Home Directory screen appears.

5. Select **Create a new Middleware Home** and identify the desired location for your new Middleware Home directory, which is the top-level directory for all Oracle Fusion Middleware products. The WebLogic Home directory will be created inside the Middleware Home directory.

> **Note:** If the Middleware Home directory already exists on your system, it must be an empty directory.

Click **Next**. The Register for Security Updates screen appears.

6. Select whether or not you want to receive the latest product and security updates. If you choose not to receive anything, you will be asked to verify your selection before continuing.

Click **Next**. The Choose Install Type screen appears.

7. Select **Typical** and click **Next**. The Choose Product Installation Directories screen appears.

8. Specify the desired location for your WebLogic Server Home directory and click **Next**.

If you are installing Oracle WebLogic Server on a UNIX system, the Installation Summary screen appears. Go to step 9 now.

If you are installing Oracle WebLogic Server on a Windows system, the Choose Shortcut Location screen appears. Specify a location where you want Windows to create a shortcut to Oracle products and click **Next**. The Installation Summary screen appears.

9. Click **Next** on the Installation Summary screen.

The Installation Progress screen appears.

10. Click **Next**. The Installation Complete screen appears.

11. De-select **Run Quickstart** and click **Done** to exit the Installer.

> **Notes:**
>
> - The same user that installed Oracle WebLogic Server must install Oracle Identity Management.
> - Do not log in to the Oracle WebLogic Server Administration Console during Oracle Identity Management installation.

4.1.3 Installing the 11.1.1.2.0 Version of Oracle Identity Management Software

Follow the instructions in Table 4–1 to install Oracle Identity Management 11.1.1.2.0.

If you need additional help with any of the installation screens, click **Help** to access the online help.

Table 4–1   Installation Flow for Install Only Option

No.	Screen	Description and Action Required
1	Welcome Screen	Click **Next** to continue.
2	Select Installation Type Screen	Select **Install Software - Do Not Configure**.
		Click **Next** to continue.
3	Prerequisite Checks Screen	Click **Next** to continue.
4	Specify Installation Location Screen	Specify the Middleware Home and Oracle Home locations.
		For more information about these directories, see "Oracle Fusion Middleware Directory Structure and Concepts" in *Oracle Fusion Middleware Installation Planning Guide*.
		Click **Next** to continue.
5	Specify Security Updates Screen	Provide your E-mail address to be informed of the latest product issues.
		Click **Next** to continue.
6	Installation Summary Screen (Install Only Option)	Verify the information on this screen.
		Click **Install** to begin the installation.
7	Installation Progress Screen	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.
		Click **Next** to continue.
8	Installation Complete Screen	Click **Finish** to dismiss the installer.

Oracle Identity Management 11*g* Release 1 (11.1.1.2.0) is installed. By default Oracle_IDM1 is created as the Oracle Identity Management Oracle home directory. You must patch this installation to 11.1.1.4.0

4.1.4 Patching the Oracle Identity Management 11.1.1.2.0 to 11.1.1.4.0

After the Oracle Identity Management 11.1.1.2.0 installation is complete, you must run the Patch Set Installer for Oracle Identity Management to update your 11.1.1.2.0 software to 11.1.1.4.0

To patch Oracle Identity Management 11*g* Release 1 (11.1.1.2.0) installation do the following:

1. Ensure that you have installed Oracle WebLogic Server 11*g* (10.3.4) on your machine.

> **Note:**   If you are installing Oracle Internet Directory 11*g* Release 1 (11.1.1.4.0) without an Oracle WebLogic administration domain, you do not need to install Oracle WebLogic.

2. Ensure that Oracle Identity Management 11*g* Release 1 (11.1.1.4.0) Patch Set Installer (ofm_idm_win_11.1.1.4.0_32_disk1_1of1.zip (for **Windows**) or ofm_idm_linux_11.1.1.4.0_32_disk1_1of1.zip (for **Linux**)) is downloaded to your machine where Oracle Identity Management 11*g* Release 1 (11.1.1.2.0) is installed.

3. Extract the contents of the file `ofm_idm_win_11.1.1.4.0_32_disk1_`
   `1of1.zip` (for **Windows**) or `ofm_idm_linux_11.1.1.4.0_32_disk1_`
   `1of1.zip` (for **Linux**) to a local directory.

4. Run `setup.exe` (for **Windows**) or `./runInstaller` (for **UNIX**) from the Disk1
   directory.

   The Welcome screen of the Oracle Identity Management 11*g* Release 1 (11.1.1.4.0)
   Patch Set Installer is displayed.

   Click **Next** to continue.

5. Specify Installation Location Screen appears. Specify the location of the Oracle
   Identity Management 11*g* Release 1 (11.1.1.2.0) Oracle Identity Management
   Oracle home directory.

   Click **Next** to continue.

6. The Security Updates Screen appears. Provide your E-mail address to be informed
   of the latest product issues.

   Click **Next** to continue.

7. The Installation Summary Screen appears. Verify the information on this screen.

   Click **Install** to begin the installation.

8. The Installation Progress Screen appears.

   Click **Next** to continue.

9. The Installation Complete Screen appears.

   Click **Finish** to dismiss the installer.

> **Note:** For detailed instructions, go to "Applying the Latest Oracle
> Fusion Middleware Patch Set with the Patch Set Installers" in *Oracle
> Fusion Middleware Patching Guide*

Oracle Identity Management 11*g* Release 1 (11.1.1.2.0) is patched to Oracle Identity
Management 11*g* Release 1 (11.1.1.4.0). You are now ready to configure your Oracle
Identity Management 11*g* Release 1 (11.1.1.4.0) components:

- Oracle Internet Directory (OID)

- Oracle Virtual Directory (OVD)

- Oracle Directory Services Manager (ODSM)

- Oracle Directory Integration Platform (ODIP)

- Oracle Identity Federation (OIF)

4.1.5 Configuring Your Components

After you have patched your software to the latest version, you are ready to configure
the following components:

- Oracle Internet Directory (OID)

- Oracle Virtual Directory (OVD)

- Oracle Directory Services Manager (ODSM)

- Oracle Directory Integration Platform (ODIP)

- Oracle Identity Federation (OIF)

You must run the Oracle Identity Management Configuration Wizard to create your WebLogic Domain and configure your components.

On UNIX systems:

```
ORACLE_HOME/bin/config.sh
```

On Windows systems:

```
ORACLE_HOME\bin\config.bat
```

The Oracle Identity Management 11*g* Configuration Wizard is displayed. You can use this wizard to configure your component in a new domain, in an existing domain, or without a domain. Note that you can install and configure only Oracle Internet Directory and Oracle Virtual Directory without a domain. For more information, see the following topics:

- OID with ODIP, ODSM, and Fusion Middleware Control in a New WebLogic Domain
- Only OID Without a WebLogic Domain
- OVD with ODSM and Fusion Middleware Control in a New WebLogic Domain
- OIF with OID in a New WebLogic Domain for LDAP Authentication, User Store, and Federation Store

4.2 OID with ODIP, ODSM, and Fusion Middleware Control in a New WebLogic Domain

This topic describes how to configure Oracle Internet Directory (OID) with Oracle Directory Integration Platform (ODIP), Oracle Directory Services Manager (ODSM), and Fusion Middleware Control in a new WebLogic administration domain. It includes the following sections:

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure

4.2.1 Appropriate Deployment Environment

The configuration described in this topic is appropriate for environments that have *both* of the following conditions:

- You want to install Oracle Internet Directory and Oracle Directory Integration Platform colocated on the same host.
- There is no WebLogic Administration Server managing other 11g Release 1 (11.1.1) Oracle Directory Services components.

4.2.2 Components Deployed

Performing the configuration in this section deploys the following components:

- WebLogic Administration Server
- Oracle Internet Directory

- WebLogic Managed Server
- Oracle Directory Integration Platform
- Oracle Directory Services Manager
- Fusion Middleware Control

4.2.3 Dependencies

The configuration in this section depends on the following:

- Oracle WebLogic Server
- Oracle Database
- If you want to use an existing schema, *Identity Management - Oracle Internet Directory* schema existing in the Oracle Database.

4.2.4 Procedure

Perform the following steps to configure Oracle Internet Directory with Oracle Directory Integration Platform, Oracle Directory Services Manager, and Fusion Middleware Control in a new domain:

1. Ensure that Oracle Internet Directory is installed, as described in Installing and Configuring OID, OVD, ODSM, ODIP, and OIF (11.1.1.4.0).

2. Run `<ORACLE_HOME>/bin/config.sh` (On UNIX) or `<ORACLE_HOME>\bin\config.bat` to start the Oracle Identity Management Configuration Wizard. Click **Next** to continue.

3. On the Select Domain screen, select **Create New Domain** and enter the following information:

   - Enter the user name for the new domain in the User Name field.
   - Enter the user password for the new domain in the User Password field.
   - Enter the user password again in the Confirm Password field.
   - Enter a name for the new domain in the Domain Name field.

   Click **Next**. The Specify Installation Location screen appears.

4. Identify the Homes, Instances, and the WebLogic Server directory by referring to Identifying Installation Directories. After you enter information for each field, click **Next.** The Specify Security Updates screen appears.

5. Choose how you want to be notified about security issues:

   - If you want to be notified about security issues through email, enter your email address in the Email field.
   - If you want to be notified about security issues through My Oracle Support (formerly MetaLink), select the My Oracle Support option and enter your My Oracle Support Password.
   - If you do not want to be notified about security issues, leave all fields empty.

   Click **Next**. The Configure Components screen appears.

6. Select **Oracle Internet Directory** and **Oracle Directory Integration Platform**. The **Oracle Directory Services Manager** and **Oracle Fusion Middleware Control** will be automatically selected.

Ensure no other components are selected and click **Next**. The Configure Ports screen appears.

7. Choose how you want the Installer to configure ports:

   - Select **Auto Port Configuration** if you want the Installer to configure ports from a predetermined range.

   - Select **Specify Ports using Configuration File** if you want the Installer to configure ports using the staticports.ini file. You can click **View/Edit File** to update the settings in the staticports.ini file.

   Click **Next**. The Specify Schema Database screen appears.

8. Choose whether to use an existing schema or to create a new one using the Installer.

Note: If you want to use an existing schema, it must currently reside in the database to continue with the installation. If it does not currently reside in the database, you must create it now using the Oracle Fusion Middleware Oracle Fusion Middleware Repository Creation Utility or follow the To create a new schema section mentioned below.

Refer to Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU) for more information.

To use an existing schema:

   a. Select **Use Existing Schema**.

   b. Enter the database connection information in the Connect String field. The connection string must be in the form: *hostname:port:servicename*. For Oracle Real Application Clusters (RAC), the connection string must be in the form: *hostname1:port1:instance1^hostname2:port2:instance2@servicename*.

   c. Enter the password for the existing ODS schema in the Password field.

   d. Click **Next**.

Note: If your existing ODS and ODSSM schemas have different passwords, the Specify ODSSM Password screen will appear after you click **Next**. Enter the password for your existing ODSSM schema and click **Next**.

The Create Oracle Internet Directory screen appears.

   e. Continue the installation by going to step 9 now.

To create a new schema

   a. Select **Create Schema**.

   b. Enter the database connection information in the Connect String field. The connection string must be in the form: *hostname:port:servicename*. For Oracle Real Application Clusters (RAC), the connection string must be in the form: *hostname1:port1:instance1^hostname2:port2:instance2@servicename*.

   c. Enter the name of the database user in the User Name field. The user you identify must have DBA privileges.

     d. Enter the password for the database user in the Password field.

     e. Click **Next**. The Enter OID Passwords screen appears.

     f. Create a password for the new ODS schema by entering it in the ODS Schema Password field.

     Enter it again in the Confirm ODS Schema Password field.

     g. Create a password for the new ODSSM schema by entering it in the ODSSM Schema Password field.

     Enter it again in the Confirm ODSSM Schema Password field.

     h. Click **Next**. The Create Oracle Internet Directory screen appears.

9. Enter the following information for Oracle Internet Directory:

- Realm: Enter the location for your realm.

- Administrator Password: Enter the password for the Oracle Internet Directory administrator.

- Confirm Password: Enter the administrator password again.

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

10. Complete the installation by performing all the steps in Completing an Installation.

Note: You may see the following error message in `$Instance_home/diagnostics/logs/OID/oid1/**` log files after configuring Oracle Internet Directory:

```
"2010-02-01T07:27:42+00:00] [OID] [NOTIFICATION:16]
[] [OIDLDAPD] [host:stadp47] [pid: 26444] [tid: 0]
Main:: FATAL * gslsmaiaInitAudCtx * Audit struct
initialization failed. Audit error code: 62005"
```

You can ignore this error message.

4.3 Only OID Without a WebLogic Domain

This topic describes how to configure only Oracle Internet Directory (OID) without a WebLogic administration domain. It includes the following sections:

- Appropriate Deployment Environment

- Components Deployed

- Dependencies

- Procedure

4.3.1 Appropriate Deployment Environment

The configuration described in this topic is appropriate for environments that have *both* of the following conditions:

- You do not want to include Oracle Internet Directory in a WebLogic administration domain for management purposes.

- You do not want to manage Oracle Internet Directory using Fusion Middleware Control.

4.3.2 Components Deployed

Performing the configuration in this section deploys only Oracle Internet Directory.

4.3.3 Dependencies

The configuration in this section depends on the following:

- Oracle Database

- If you want to use an existing schema, *Identity Management - Oracle Internet Directory* schema existing in the Oracle Database.

4.3.4 Procedure

Perform the following steps to configure only Oracle Internet Directory without a domain:

1. Ensure that Oracle Internet Directory is installed, as described in Installing and Configuring OID, OVD, ODSM, ODIP, and OIF (11.1.1.4.0).

   Note that installing Oracle WebLogic Server is optional in this particular scenario. Instead, you can create the Middleware Home by using the Oracle Identity Management Configuration Wizard, as described later in Step 4 of the procedure.

2. Run `<ORACLE_HOME>/bin/config.sh` (On UNIX) or `<ORACLE_HOME>\bin\config.bat` to start the Oracle Identity Management Configuration Wizard. Click **Next** to continue.

3. Select **Configure without a Domain** on the Select Domain screen and click **Next**. The Specify Installation Location screen appears.

4. Enter the following information in each field:

   - **Oracle Middleware Home Location**: If an Oracle Middleware Home directory already exists, enter the path to it in this field. If an Oracle Middleware Home directory *does not* exist, enter a path to the location where you want the Installer to create the directory that will contain the Oracle Common Home and Oracle Home directories. The Installer creates an Oracle Common Home directory and an Oracle Home directory inside the directory you identify in this field.

     The Oracle Middleware Home directory is commonly referred to as *MW_HOME*.

   > **Note:** The Oracle Middleware Home directory is *not* required to contain an Oracle WebLogic Server installation.

   - **Oracle Home Directory**: Enter a name for the Oracle Home directory. 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 Oracle Home directory is commonly referred to as *ORACLE_HOME*.

   - **Oracle Instance Location**: Enter the directory path to the location where you want to create the Oracle Instance directory. The Installer creates the Oracle Instance directory using the location you enter in this field and using the name you enter in the Oracle Instance Name field. You can identify any location on

your system for the Oracle Instance directory—it does not have to reside inside the Oracle Middleware Home directory.

- **Oracle Instance Name**: Enter a name for the Oracle Instance directory. The Installer uses the name you enter in this field to create the Oracle Instance directory at the location you specify in the Oracle Instance Location field. This directory is commonly referred to as *ORACLE_INSTANCE*.

After you enter information for each field, click **Next.** The Specify Security Updates screen appears.

5. Choose how you want to be notified about security issues:

- If you want to be notified about security issues through email, enter your email address in the Email field.

- If you want to be notified about security issues through My Oracle Support (formerly MetaLink), select the My Oracle Support option and enter your My Oracle Support Password.

- If you do not want to be notified about security issues, leave all fields empty.

Click **Next**. The Configure Components screen appears.

6. On the Configure Components screen, select only **Oracle Internet Directory**. Ensure no other components are selected and click **Next**. The Configure Ports screen appears.

7. Choose how you want the Installer to configure ports:

- Select **Auto Port Configuration** if you want the Installer to configure ports from a predetermined range.

- Select **Specify Ports using Configuration File** if you want the Installer to configure ports using the staticports.ini file. You can click **View/Edit File** to update the settings in the staticports.ini file.

Click **Next**. The Specify Schema Database screen appears.

8. Choose whether to use an existing schema or to create a new one using the Installer.

Note: If you want to use an existing schema, it must currently reside in the database to continue with the installation. If it does not currently reside in the database, you must create it now using the Oracle Fusion Middleware Repository Creation Utility or follow the To create a new schema section mentioned below.

Refer to Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU) for more information.

To use an existing schema:

a. Select **Use Existing Schema**.

b. Enter the database connection information in the Connect String field. The connection string must be in the form: *hostname:port:servicename*. For Oracle Real Application Clusters (RAC), the connection string must be in the form: *hostname1:port1:instance1^hostname2:port2:instance2@servicename*.

c. Enter the password for the existing ODS schema in the Password field.

d. Click **Next**.

> **Note:** If your existing ODS and ODSSM schemas have different passwords, the Specify ODSSM Password screen will appear after you click **Next**. Enter the password for your existing ODSSM schema and click **Next**.

        The Create Oracle Internet Directory screen appears.

  e. Continue the installation by going to step 9 now.

To create a new schema

  a. Select **Create Schema**.

  b. Enter the database connection information in the Connect String field. The connection string must be in the form: *hostname*:*port*:*servicename*. For Oracle Real Application Clusters (RAC), the connection string must be in the form: *hostname1*:*port1*:*instance1^hostname2*:*port2*:*instance2@servicename*.

  c. Enter the name of the database user in the User Name field. The user you identify must have DBA privileges.

  d. Enter the password for the database user in the Password field.

  e. Click **Next**. The Enter OID Passwords screen appears.

  f. Create a password for the new ODS schema by entering it in the ODS Schema Password field.

      Enter it again in the Confirm ODS Schema Password field.

  g. Create a password for the new ODSSM schema by entering it in the ODSSM Schema Password field.

      Enter it again in the Confirm ODSSM Schema Password field.

  h. Click **Next**. The Create Oracle Internet Directory screen appears.

9. Enter the following information for Oracle Internet Directory:

- Realm: Enter the location for your realm.

- Administrator Password: Enter the password for the Oracle Internet Directory administrator.

- Confirm Password: Enter the administrator password again.

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

10. Complete the installation by performing all the steps in Completing an Installation.

> **Note:**
>
> - If you perform this installation and configuration, but later decide you want to manage Oracle Internet Directory using Fusion Middleware Control, you must register Oracle Internet Directory with a WebLogic Administration Server.
>
>   Refer to the "Registering an Oracle Instance or Component with the WebLogic Server" section in the *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory* for more information.
>
> - You may see the following error message in `$Instance_home/diagnostics/logs/OID/oid1/**` log files after configuring Oracle Internet Directory:
>
>   ```
>   "2010-02-01T07:27:42+00:00] [OID]
>   [NOTIFICATION:16] [] [OIDLDAPD] [host:stadp47]
>   [pid: 26444] [tid: 0] Main:: FATAL *
>   gslsmaiaInitAudCtx * Audit struct initialization
>   failed. Audit error code: 62005"
>   ```
>
>   You can ignore this error message.

4.4 OVD with ODSM and Fusion Middleware Control in a New WebLogic Domain

This topic describes how to configure Oracle Virtual Directory (OVD) with Oracle Directory Services Manager (ODSM) and Fusion Middleware Control in a new WebLogic administration domain. It includes the following sections:

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure

4.4.1 Appropriate Deployment Environment

The configuration described in this topic is appropriate for environments that have *all* of the following conditions:

- You want to manage Oracle Virtual Directory using Fusion Middleware Control.
- You want Oracle Virtual Directory to be in a WebLogic administration domain.
- There is no WebLogic Administration Server managing other 11g Release 1 (11.1.1) Oracle Directory Services components.
- You want to install Oracle Virtual Directory and a WebLogic Administration Server colocated on the same host.

4.4.2 Components Deployed

Performing the configuration in this section deploys the following components.

- WebLogic Administration Server

- Oracle Virtual Directory

- Oracle Directory Services Manager

- Fusion Middleware Control

4.4.3 Dependencies

The configuration in this section depends on Oracle WebLogic Server.

4.4.4 Procedure

Perform the following steps to configure Oracle Virtual Directory with Oracle Directory Services Manager and Fusion Middleware Control in a new domain:

1. Ensure that Oracle Virtual Directory and Oracle Directory Services Manager are installed, as described in Installing and Configuring OID, OVD, ODSM, ODIP, and OIF (11.1.1.4.0).

2. Run `<ORACLE_HOME>/bin/config.sh` (On UNIX) or `<ORACLE_HOME>\bin\config.bat` to start the Oracle Identity Management Configuration Wizard. Click **Next** to continue.

3. On the Select Domain screen, select **Create New Domain** and enter the following information:

   - Enter the user name for the new domain in the User Name field.

   - Enter the user password for the new domain in the User Password field.

   - Enter the user password again in the Confirm Password field.

   - Enter a name for the new domain in the Domain Name field.

   Click **Next**. The Specify Installation Location screen appears.

4. Identify the Homes, Instances, and the WebLogic Server directory by referring to Identifying Installation Directories. After you enter information for each field, click **Next.** The Specify Security Updates screen appears.

5. Choose how you want to be notified about security issues:

   - If you want to be notified about security issues through email, enter your email address in the Email field.

   - If you want to be notified about security issues through My Oracle Support (formerly MetaLink), select the My Oracle Support option and enter your My Oracle Support Password.

   - If you do not want to be notified about security issues, leave all fields empty.

   Click **Next**. The Configure Components screen appears.

6. Select only **Oracle Virtual Directory**. The Oracle Directory Services Manager and Fusion Middleware Control management components are automatically selected for this installation.

   Ensure no other components are selected and click **Next**. The Configure Ports screen appears.

7. Choose how you want the Installer to configure ports:

   - Select **Auto Port Configuration** if you want the Installer to configure ports from a predetermined range.

- Select **Specify Ports using Configuration File** if you want the Installer to configure ports using the staticports.ini file. You can click **View/Edit File** to update the settings in the staticports.ini file.

  Click **Next**. The Specify Oracle Virtual Directory Information screen appears.

8. Enter the following information:

   - LDAP v3 Name Space: Enter the name space for Oracle Virtual Directory. The default value is dc=us,dc=oracle,dc=com.

   - HTTP Web Gateway: Select this option to enable the Oracle Virtual Directory HTTP Web Gateway.

   - Secure: Select this option if you enabled the HTTP Web Gateway and you want to secure it using SSL.

   - Administrator User Name: Enter the user name for the Oracle Virtual Directory administrator. The default value is cn=orcladmin.

   - Password: Enter the password for the Oracle Virtual Directory administrator.

   - Confirm Password: Enter the password for the Oracle Virtual Directory administrator again.

   - Configure Administrative Server in secure mode: Select this option to secure the Oracle Virtual Directory Administrative Listener using SSL. This option is selected by default. Oracle recommends selecting this option.

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

9. Complete the installation by performing all the steps in Completing an Installation.

4.4.5 Post-Configuration Task

After configuring Oracle Virtual Directory, you must complete the following task to update the Oracle Virtual Directory Version Number in Oracle Directory Service Manager:

1. Set the `JAVA_HOME` and `ANT_HOME` environment variables and add them to the PATH environment variable.

2. Go to the `ORACLE_HOME/ovd/patchset` (on UNIX operating systems) or `ORACLE_HOME\ovd\patchset` (on Windows operating systems) directory and run the following command:

   ```
   ant updateOVDVersion -Dovd_instance=<ovd_instance_location>
   ```

3. Restart the Oracle Virtual Directory instance.

4.5 OIF with OID in a New WebLogic Domain for LDAP Authentication, User Store, and Federation Store

This section describes how to configure Oracle Identity Federation (OIF) with Oracle Internet Directory (OID) in a new WebLogic administration domain for LDAP Authentication, User Store, and Federation Store.

> **Note:** When you configure Oracle Identity Federation with Oracle Internet Directory, the Installer automatically configures connection, credential, attribute, and container settings using the Oracle Internet Directory configuration.

This section includes the following information about this configuration:

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure

4.5.1 Appropriate Deployment Environment

Perform the configuration in this topic to quickly deploy Oracle Identity Federation with Oracle Internet Directory as the LDAP repository for Authentication, User Store, and Federation Store.

4.5.2 Components Deployed

Performing the configuration in this section deploys the following components:

- WebLogic Managed Server
- Oracle Identity Federation
- Oracle Internet Directory
- Oracle Directory Services Manager
- WebLogic Administration Server
- Fusion Middleware Control
- *Optionally*, Oracle HTTP Server

4.5.3 Dependencies

The configuration in this section depends on the following components:

- Oracle WebLogic Server
- Oracle Database for Oracle Internet Directory
- *Identity Management - Oracle Internet Directory* schema existing in the database for Oracle Internet Directory.
- Oracle Database for Oracle Identity Federation, if using RDBMS for Session Store, Message Store, or Configuration Store.
- New *Identity Management - Oracle Identity Federation* schema existing in the database for Oracle Identity Federation, if using RDBMS for Session Store, Message Store, or Configuration Store.

4.5.4 Procedure

Perform the following steps to configure Oracle Identity Federation with Oracle Internet Directory in a new domain for LDAP Authentication, User Store, and Federation Store:

1. Decide if you want to use RDBMS for Session Store, Message Store, or Configuration Store. If you do, perform the following steps a and b:

   a. Install the database for Oracle Identity Federation. Refer to Installing Oracle Database for more information.

   b. Create the *Identity Management - Oracle Identity Federation* schema in the database. Refer to Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU) for more information.

2. Install the Oracle Database for Oracle Internet Directory. Refer to Installing Oracle Database for more information.

3. Create the *Identity Management - Oracle Internet Directory* schema in the database for Oracle Internet Directory. Refer to Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU) for more information.

4. Ensure that Oracle Identity Federation and Oracle Internet Directory are installed, as described in Installing and Configuring OID, OVD, ODSM, ODIP, and OIF (11.1.1.4.0).

5. Run `<ORACLE_HOME>/bin/config.sh` (On UNIX) or `<ORACLE_HOME>\bin\config.bat` to start the Oracle Identity Management Configuration Wizard. Click **Next** to continue.

6. On the Select Domain screen, select **Create New Domain** and enter the following information:

   - User Name: Enter the user name for the new domain.

   - User Password: Enter the user password for the new domain.

     Enter the user password again in the Confirm Password field.

   - Domain Name: Enter a name for the new domain.

   Click **Next**. The Specify Installation Location screen appears.

7. Identify the Homes, Instances, and the WebLogic Server directory by referring to Identifying Installation Directories. After you enter information for each field, click **Next.** The Specify Security Updates screen appears.

8. Choose how you want to be notified about security issues:

   - If you want to be notified about security issues through email, enter your email address in the Email field.

   - If you want to be notified about security issues through My Oracle Support (formerly MetaLink), select the My Oracle Support option and enter your My Oracle Support Password.

   - If you do not want to be notified about security issues, leave all fields empty.

   Click **Next**. The Configure Components screen appears.

9. Select **Oracle Internet Directory**, **Oracle Identity Federation**, and *optionally*, **Oracle HTTP Server**.

> **Note:** Oracle HTTP Server is required when using Oracle Identity Federation for enterprise level single sign-on with Oracle Single Sign-On and Oracle Access Manager. Although Oracle Identity Federation can function without Oracle HTTP Server, there are advantages to configuring it as a proxy for Oracle Identity Federation.
>
> When you select Oracle HTTP Server and Oracle Identity Federation on this Configure Components screen, the Configuration Wizard configures the Oracle HTTP Server so that the Oracle Identity Federation application can be accessed through Oracle HTTP Server ports.
>
> Refer to the "Deploying Oracle Identity Federation with Oracle HTTP Server" section in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation* for more information.

The Oracle Directory Services Manager and Fusion Middleware Control management components are automatically selected for this installation.

Ensure no other components are selected and click **Next**. The Configure Ports screen appears.

10. Choose how you want the Installer to configure ports:

   - Select **Auto Port Configuration** if you want the Installer to configure ports from a predetermined range.

   - Select **Specify Ports using Configuration File** if you want the Installer to configure ports using the staticports.ini file. You can click **View/Edit File** to update the settings in the staticports.ini file.

   Click **Next**. The Specify Schema Database screen appears.

11. Identify the ODS schema for Oracle Internet Directory that you created in step 3 by selecting **Use Existing Schema** and entering the following information:

   - Enter the database connection information in the Connect String field. The connection string must be in the form: *hostname:port:servicename*. For Oracle Real Application Clusters (RAC), the connection string must be in the form: *hostname1:port1:instance1^hostname2:port2:instance2@servicename*.

   - Enter the password for the ODS schema in the Password field and click **Next**.

> **Note:** If your existing ODS and ODSSM schemas have different passwords, the Specify ODSSM Password screen will appear after you click **Next**. Enter the password for your existing ODSSM schema and click **Next**.

The Create Oracle Internet Directory screen appears.

12. Enter the following information for Oracle Internet Directory:

   - Realm: Enter the location for your realm.

   - Administrator Password: Enter the password for the Oracle Internet Directory administrator.

   - Confirm Password: Enter the administrator password again.

   Click **Next**. The Specify OIF Details screen appears.

13. Enter the following information:

- PKCS12 Password: Enter the password Oracle Identity Federation will use for encryption and for signing wallets. The Installer automatically generates these wallets with self-signed certificates. Oracle recommends using the wallets only for testing.

- Confirm Password: Enter the PKCS12 password again.

- Server ID: Enter a string that will be used to identify this Oracle Identity Federation instance. A prefix of `oif` will be added to the beginning of the string you enter. Each logical Oracle Identity Federation instance within an Oracle WebLogic Server administration domain must have a unique Server ID. Clustered Oracle Identity Federation instances acting as a single logical instance will have the same Server ID.

Click **Next**. The Select OIF Advanced Flow Attributes screen appears.

> **Notes:**
>
> - Notice that the options for Authentication Type, User Store and Federation Store are automatically set to LDAP because you are installing Oracle Internet Directory with Oracle Identity Federation.
>
> - The Installer sets the User Federation Record Context to cn=fed,*BASE_REALM*, where *BASE_REALM* is typically dc=us,dc=oracle,dc=com.

14. Select the appropriate option for each configuration item and click **Next**:

> **Note:** User Session Store and Message Store appear in the Installer as separate configuration items, however, most deployments use the same type of repository for both stores.

- User Session Store: **Memory** or **RDBMS**

  – Select Memory to store transient runtime session state data in in-memory tables.

  – Select RDBMS to store transient runtime session state data in a relational database.

- Message Store: **Memory** or **RDBMS**

  – Select Memory to store transient protocol messages in in-memory tables

  – Select RDBMS to store transient protocol messages in a relational database.

- Configuration Store: **File** or **RDBMS**

  – Select File to store Oracle Identity Federation configuration data on the local file system.

  – Select RDBMS to store Oracle Identity Federation configuration data in a relational database.

> **Note:** The screens that appear next depend on the options you selected for the configuration items.
>
> - If you selected RDBMS for User Session Store, Message Store, or Configuration Store, go to step 15 now.
>
> - If you did *not* select RDBMS for User Session Store, Message Store, or Configuration Store, go to step 16 now.

15. Enter the following information on the Specify Transient Store Database Details screen:

    - HostName: Enter the connection string to the database host in the form: *hostname:port:servicename*. For Oracle Real Application Clusters (RAC), the connection string must be in the form: *hostname1:port1:instance1^hostname2:port2:instance2@servicename*.

    - Username: Enter the name of the schema owner created by RCU, which is of the form *PREFIX_OIF*.

    - Password: Enter the password for the database user.

16. Complete the installation by performing all the steps in Completing an Installation.

> **Note:** To configure Oracle Identity Federation so that it is integrated with Oracle HTTP Server, refer to the "Deploying Oracle Identity Federation with Oracle HTTP Server" section in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*.

5

Installing and Configuring OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0)

This chapter includes the following topics:

- Installing OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0)
- After Installing the Oracle Identity Management Software
- Basic Installation and Configuration Scenarios
- Configuring OIM Server, Design Console, and Remote Manager
- Oracle Identity Management Suite-Level Installation Scenarios
- Installing Oracle HTTP Server 11g WebGate for OAM
- Setting Up Integration Between OIM and OAM

5.1 Installing OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0)

This section describes how to install the Oracle Identity Management 11*g* Release 1 (11.1.1.3.0) suite that contains the following products:

- Oracle Identity Manager (OIM)
- Oracle Access Manager (OAM)
- Oracle Adaptive Access Manager (OAAM)
- Oracle Authorization Policy Manager (OAPM)
- Oracle Identity Navigator (OIN)

It includes the following sections:

- Applications Installed
- Dependencies
- Procedure

5.1.1 Applications Installed

Performing the installation in this section installs the following products:

- Oracle Identity Manager Server
- Oracle Identity Manager Design Console
- Oracle Identity Manager Remote Manager

- Oracle Access Manager

- Oracle Adaptive Access Manager

- Oracle Identity Navigator

- Oracle Authorization Policy Manager

5.1.2 Dependencies

The installation in this section depends on the following:

- Oracle WebLogic Server

- Oracle Database

- Oracle SOA 11*g* Suite 11.1.1.3.0 (required for Oracle Identity Manager only)

- JDK (either Oracle WebLogic JRockit JDK or Sun JDK 1.6.0)

5.1.3 Procedure

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

1. Install the Oracle Database. Refer to Installing Oracle Database for more information.

   > **Note:** Ensure that the Oracle database is with the AL32UTF8 character set encoding.

2. Decide if you want to create new schemas for Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Metadata Services, and SOA Infrastructure by using the Installer during installation or if you want to use an existing schema:

   - If you want to create a new schema using the Installer, refer to Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU) for more information about creating schemas. After creating schemas, continue this procedure by going to Step 3.

   - If you want to use an existing schema, you must upgrade the schema by using the Upgrade Assistant tool. For more information, see the *Oracle Fusion Middleware Upgrade Guide for Oracle Identity Management*.

3. Install Oracle WebLogic Server. Refer to Installing Oracle WebLogic Server 10.3.3 and Creating the Oracle Middleware Home for more information.

4. Install Oracle SOA 11*g* suite (11.1.1.3.0) if you want to use Oracle Identity Manager. For information about installing the Oracle SOA 11*g* suite, refer to Installing the Latest Version of Oracle SOA Suite (Oracle Identity Manager Users Only).

5. Start your installation by performing all the steps in Starting an Installation. After you complete those steps, the Welcome screen appears.

6. Click **Next** on the Welcome screen. The Prerequisite Checks screen appears.

7. If all prerequisite checks pass inspection, click **Next**. The Specify Installation Location screen appears.

8. 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 verifies 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 on a Windows machine, you do not need to install Oracle WebLogic Server and create a Middleware Home directory on the Windows machine. Before using Oracle Identity Manager Design Console, you must configure Oracle Identity Manager Server. However, the Server can be installed and configured on a different machine, so you can specify the Oracle Identity Manager Server host and URL information when configuring only Design Console on the Windows machine.

9. 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 IDM_Home in this book.

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

   The 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 Oracle Identity Management, click **Install**.

   This installation process copies the Identity Management software to your system and creates an IDM_Home directory, such as Oracle_IDM1, under your Middleware Home. You must proceed to create a WebLogic Domain, as described in After Installing the Oracle Identity Management Software. In addition, you must configure the Administration Server settings while creating the domain.

   To configure Oracle Identity Manager Server, Oracle Identity Manager Design Console, and Oracle Identity Manager Remote Manager, you must launch the Oracle Identity Manager 11*g* Configuration Wizard, as described in Starting the Oracle Identity Manager 11g Configuration Wizard.

   In addition, see Configuring OIM Server, Configuring OIM Design Console, and Configuring OIM Remote Manager.

5.2 After Installing the Oracle Identity Management Software

After installing the Oracle Identity Management software, you must proceed to configure Oracle Identity Management products in a new or existing WebLogic domain. You can use the Oracle Fusion Middleware Configuration Wizard to create a WebLogic domain or extend an existing domain. For more information about WebLogic administration domain options, see the "Introduction to WebLogic

Domains" topic in the guide *Oracle Fusion Middleware Creating Domains Using the Configuration Wizard*.

This chapter discusses some of the basic installation and configuration scenarios. For more information about advanced installation scenarios, including Oracle Identity Management suite-level scenarios, see the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

> **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.

For Oracle Identity Manager users only:

After configuring Oracle Identity Manager in a new or existing WebLogic domain, you must configure Oracle Identity Manager Server, Oracle Identity Manager Design Console, and Oracle Identity Manager Remote Manager, by running the Oracle Identity Manager 11*g* Configuration Wizard, as described in Configuring OIM Server, Design Console, and Remote Manager.

5.3 Basic Installation and Configuration Scenarios

This section includes some of the most basic installation and configuration scenarios for Oracle Identity Management 11*g* Release 1 (11.1.1.3.0) products, comprising Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Identity Navigator, and Oracle Identity Navigator.

For an extensive list of installation and configuration scenarios, including Oracle Identity Management suite-level installation scenarios, see the chapter "Oracle Identity Management Suite-Level Installation Scenarios" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management.*

This section discusses the following topics:

- OIN in a New WebLogic Domain
- OIM Without LDAP Sync in a New WebLogic Domain
- OIM with LDAP Sync
- OIM with LDAP Sync, and OAM
- OAM in a New WebLogic Domain
- OAAM in a New WebLogic Domain
- OAPM in a New WebLogic Domain
- OAPM in a Domain Containing OIM, OAM, OAAM, and OIN

5.3.1 OIN in a New WebLogic Domain

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

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure

5.3.1.1 Appropriate Deployment Environment

Perform the configuration in this topic if you want to use Oracle Identity Navigator with Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Authorization Policy 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, Oracle Adaptive Access Manager, and Oracle Authorization Policy Manager. You can then access those product consoles from within the Oracle Identity Navigator interface, without having to remember the individual console URLs.

5.3.1.2 Components Deployed

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

5.3.1.3 Dependencies

The configuration in this section depends on the following:

- Oracle WebLogic Server

- Installation of the Oracle Identity Management 11*g* software

For more information, see Preparing to Install Oracle Identity Management and Installing OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0).

5.3.1.4 Procedure

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

1. Install Oracle WebLogic Server, and create a Middleware Home, as described in Installing Oracle WebLogic Server 10.3.3 and Creating the Oracle Middleware Home.

2. Install the Oracle Identity Management 11*g* software. Refer to Installing OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0) for more information.

3. Run the `<IDM_Home>/common/bin/config.sh` script. (`<IDM_Home>\common\bin\config.cmd` on Windows). This IDM_Home is the directory where you installed Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Authorization Policy Manager, and Oracle Identity Navigator.

   The Welcome screen of the Oracle Fusion Middleware Configuration Wizard appears.

4. On the Welcome screen, select **Create a new WebLogic domain**, and click **Next**. The Select Domain Source screen appears.

5. 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**), and click **Next**. The Specify Domain Name and Location screen appears.

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

6. Enter a name and a location for the domain to be created, and click **Next**. The Configure Administrator User Name and Password screen appears.

7. Configure a user name and a password for the administrator. The default user name is weblogic. Click **Next**.

8. Choose `JRockit SDK 1.6.0_17` and Production Mode in the Configure Server Start Mode and JDK screen of the Oracle Fusion Middleware Configuration Wizard.

    The Select Optional Configuration screen appears.

9. 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**.

10. Optional: Configure the following Administration Server parameters:

    - Name

    - Listen address

    - Listen port

    - SSL listen port

    - SSL enabled or disabled

11. Optional: Configure Managed Servers, as required.

12. Optional: Configure Clusters, as required.

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

13. Optional: Assign Managed Servers to clusters, as required.

14. 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.

15. Optional: Assign the Administration Server to a machine.

16. Optional: Select Deployments, such as applications and libraries, and Services to target them to a particular cluster or server.

17. Optional: Configure RDBMS Security Store, as required.

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.

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.

5.3.2 OIM Without LDAP Sync in a New WebLogic Domain

This topic describes how to configure Oracle Identity Manager (OIM) without LDAP Synchronization in a new WebLogic domain. It includes the following sections:

- Appropriate Deployment Environment

- Components Deployed

- Dependencies

■ Procedure

5.3.2.1 Appropriate Deployment Environment

Perform the configuration in this topic if you want to install only Oracle Identity Manager in an environment where you may use Oracle Identity Manager as a provisioning or request solution.

5.3.2.2 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

5.3.2.3 Dependencies

The configuration in this section depends on the following:

■ Oracle WebLogic Server.

■ Installation of the Oracle Identity Management 11*g* software.

■ Installation of the latest version of Oracle SOA Suite.

■ Database schemas for Oracle Identity Manager and Oracle SOA 11*g* Suite. For more information, see Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU).

5.3.2.4 Procedure

Complete the following steps to configure Oracle Identity Manager (without LDAP Sync) in a new WebLogic domain and to configure Oracle Identity Manager Server, Design Console, and Remote Manager:

1. Install Oracle WebLogic Server and create a Middleware Home, as described in Installing Oracle WebLogic Server 10.3.3 and Creating the Oracle Middleware Home.

2. Create and load the appropriate schemas required by Oracle Identity Manager and Oracle SOA Suite, as described in Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU).

3. Install the Oracle Identity Management 11*g* software. Refer to Installing OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0) for more information.

4. Install Oracle SOA Suite under the same Middleware Home, as described in Installing the Latest Version of Oracle SOA Suite (Oracle Identity Manager Users Only).

5. Run the `<IDM_Home>/common/bin/config.sh` script (on UNIX). (`<IDM_Home>\common\bin\config.cmd` on Windows). This IDM_Home is the directory where you installed Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Authorization Policy Manager, and Oracle Identity Navigator.

   The Welcome screen of the Oracle Fusion Middleware Configuration Wizard appears.

6. On the Welcome screen, select **Create a new WebLogic domain**, and click **Next**. The Select Domain Source screen appears.

7. 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**. The **Oracle SOA Suite - 11.1.1.1.0 [Oracle_SOA1]** option, the **Oracle JRF 11.1.1.0 [oracle_common]** option, the **Oracle Enterprise Manager - 11.1.1.0 [oracle_common]**, and the **Oracle WSM Policy Manager 11.1.1.0 [oracle_common]** option are also selected, by default.

Click **Next**. The Specify Domain Name and Location screen appears.

8. Enter a name and a location for the domain to be created, and click **Next**. The Configure Administrator User Name and Password screen appears.

9. Configure a user name and a password for the administrator. The default user name is weblogic. Click **Next**.

10. Choose `JRockit SDK 1.6.0_17` and Production Mode in the Configure Server Start Mode and JDK screen of the Oracle Fusion Middleware Configuration Wizard. 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

11. On the Configure JDBC Component Schema screen, select a component schema that you want to modify. You can set values for Schema Owner, Schema Password, Database and Service, Host Name, and Port. Select the driver as **Oracle's Driver (Thin) for Instance connections; Versions:9.0.1,9.2.0,10,11**. Click **Next**. The Test JDBC Component Schema screen appears. After the test succeeds, the Select Optional Configuration screen appears.

12. 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**.

13. Optional: Configure the following Administration Server parameters:

- Name
- Listen address
- Listen port
- SSL listen port
- SSL enabled or disabled

Click **Next**.

14. Optional: Configure JMS Distributed Destination, as required. Click **Next**.

15. Optional: Configure Managed Servers, as required. Click **Next**.

16. Optional: Configure Clusters, as required. For more information about configuring clusters for Oracle Identity Management products, see the "Configuring High

Availability for Identity Management Components" topic in the guide *Oracle Fusion Middleware High Availability Guide*.

Click **Next**.

17. Optional: Assign Managed Servers to Clusters, as required. Click **Next**.

18. 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**.

19. Optional: Assign servers to machines. Click **Next**.

20. Optional: Select Deployments, such as applications and libraries, and Services to target them to a particular cluster or server. Click **Next**.

21. 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.

22. Start the Administration Server, as described in Starting the Stack.

23. Configure the Oracle Identity Manager Server, Design Console, or Remote Manager, as described in Configuring OIM Server, Design Console, and Remote Manager.

5.3.3 OIM with LDAP Sync

This topic describes how to configure Oracle Identity Manager (OIM) with LDAP Synchronization in a new or existing WebLogic domain. It includes the following sections:

- OIM with LDAP Sync in a New WebLogic Domain

- OIM with LDAP Sync in a Domain Containing OID and OVD

5.3.3.1 OIM with LDAP Sync in a New WebLogic Domain

This section discusses the following topics:

- Appropriate Deployment Environment

- Components Deployed

- Dependencies

- Procedure

5.3.3.1.1 Appropriate Deployment Environment Perform the configuration in this topic if you want to install only Oracle Identity Manager in an environment where you want to set up LDAP synchronization for Oracle Identity Manager. At a later time, you can set up integration between Oracle Identity Manager and Oracle Access Manager.

5.3.3.1.2 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

5.3.3.1.3 Dependencies The configuration in this section depends on the following:

- Oracle WebLogic Server

- Installation of the Oracle Identity Management 11*g* software

- Installation of the latest version of Oracle Internet Directory and Oracle Virtual Directory under the same Middleware Home directory or on a different machine.

- Installation of the latest version of Oracle SOA Suite

- Database schemas for Oracle Identity Manager and Oracle SOA 11*g* Suite

5.3.3.1.4 Procedure Complete the following steps to configure Oracle Identity Manager with LDAP Sync in a new WebLogic administration domain:

1. Install Oracle WebLogic Server and create a Middleware Home, as described in Installing Oracle WebLogic Server 10.3.3 and Creating the Oracle Middleware Home.

2. Create and load the appropriate schemas required by Oracle Identity Manager and Oracle SOA Suite, as described in Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU).

3. Install the Oracle Identity Management 11*g* software. Refer to Installing OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0) for more information.

4. Install Oracle SOA Suite under the same Middleware Home, as described in Installing the Latest Version of Oracle SOA Suite (Oracle Identity Manager Users Only).

5. Run the `<IDM_Home>/common/bin/config.sh` script (on UNIX). (`<IDM_Home>\common\bin\config.cmd` on Windows). This IDM_Home is the directory where you installed Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Authorization Policy Manager, and Oracle Identity Navigator.

   The Welcome screen of the Oracle Fusion Middleware Configuration Wizard appears.

6. On the Welcome screen, select **Create a new WebLogic domain**, and click **Next**. The Select Domain Source screen appears.

7. 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**.

   The **Oracle SOA Suite - 11.1.1.1.0 [Oracle_SOA1]** option, the **Oracle JRF 11.1.1.0 [oracle_common]** option, the **Oracle Enterprise Manager - 11.1.1.0 [oracle_ common]**, and the **Oracle WSM Policy Manager 11.1.1.0 [oracle_common]** option are also selected, by default.

   Click **Next**. The Specify Domain Name and Location screen appears.

8. Enter a name and a location for the domain to be created, and click **Next**. The Configure Administrator User Name and Password screen appears.

9. Configure a user name and a password for the administrator. The default user name is weblogic. Click **Next**.

10. Choose `JRockit SDK 1.6.0_17` and Production Mode in the Configure Server Start Mode and JDK screen of the Oracle Fusion Middleware Configuration Wizard. 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

11. On the Configure JDBC Component Schema screen, select a component 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.

12. 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**.

13. Optional: Configure the following Administration Server parameters:

   - Name
   - Listen address
   - Listen port
   - SSL listen port
   - SSL enabled or disabled

   Click **Next**.

14. Optional: Configure JMS Distributed Destination, as required. Click **Next**.

15. Optional: Configure Managed Servers, as required. Click **Next**.

16. Optional: Configure Clusters, as required. For more information about configuring clusters for Oracle Identity Management products, see the "Configuring High Availability for Identity Management Components" topic in the *Oracle Fusion Middleware High Availability Guide*.

   Click **Next**.

17. Optional: Assign Managed Servers to Clusters, as required. Click **Next**.

18. 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**.

19. Optional: Assign servers to machines. Click **Next**.

20. Optional: Select Deployments, such as applications and libraries, and Services to target them to a particular cluster or server. Click **Next**.

21. 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.

22. Start the Administration Server, as described in Starting the Stack.

23. Set up LDAP Synchronization, as described in the "Setting Up LDAP Synchronization" topic in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

24. Configure the Oracle Identity Manager Server, Design Console, or Remote Manager, as described in Configuring OIM Server, Design Console, and Remote Manager.

5.3.3.2 OIM with LDAP Sync in a Domain Containing OID and OVD

This section discusses the following topics:

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure

5.3.3.2.1 Appropriate Deployment Environment Perform the configuration in this topic if you want to install only Oracle Identity Manager (OIM) in an existing Oracle Identity Management environment where you have installed and configured Oracle Internet Directory (OID) and Oracle Virtual Directory (OVD). You can enable LDAP Synchronization for Oracle Identity Manager. At a later time, you may install Oracle Access Manager and set up integration between Oracle Identity Manager and Oracle Access Manager.

5.3.3.2.2 Components Deployed Performing the configuration in this section installs the following components:

- 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

5.3.3.2.3 Dependencies The configuration in this section depends on the following:

- Oracle WebLogic Server
- Installation of the Oracle Identity Management 11*g* software
- Installation of the latest version of Oracle SOA Suite
- Database schemas for Oracle Identity Manager and Oracle SOA 11*g* Suite

5.3.3.2.4 Procedure Complete the following steps to configure Oracle Identity Manager with LDAP Sync in an existing Oracle Identity Management 11.1.1.3.0 domain that has Oracle Internet Directory and Oracle Virtual Directory installed and configured:

1. Install Oracle WebLogic Server and create a Middleware Home, as described in Installing Oracle WebLogic Server 10.3.3 and Creating the Oracle Middleware Home.

2. Ensure that your Oracle Identity Management 11g installation is patched to 11.1.1.3.0, as described in Installing and Configuring OID, OVD, ODSM, ODIP, and OIF (11.1.1.4.0).

3. Run the `<IDM_Home>/bin/config.sh` on UNIX operating systems to start the Oracle Identity Management Configuration Wizard. On Windows, run the `<IDM_Home>\bin\config.bat` to start the wizard. This IDM_Home is the directory where you have installed and configured Oracle Internet Directory and Oracle Virtual Directory. The Welcome screen in the Oracle Identity Management Configuration Wizard is displayed.

4. On the Select Domain screen, select the **Create New Domain** option. Set the Administrator user name and password, as required.

5. Ensure that you select **Oracle Internet Directory** and **Oracle Virtual Directory** on the Configure Components screen.

6. Follow the wizard, provide the necessary input, and configure the domain.

   A new WebLogic domain to support Oracle Internet Directory and Oracle Virtual Directory 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. Ensure that your Oracle database version is supported and you have installed the necessary patches. For more information, see Installing Oracle Database.

8. Create and load the appropriate schemas required by Oracle Identity Manager, Oracle SOA Suite, and Oracle Access Manager, as described in Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU).

9. Install the Oracle Identity Management 11*g* software under the same Middleware Home. Refer to Installing OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0) for more information. A new IDM_Home for Oracle Identity Management, such as `Oracle_IDM2`, is created under the Middleware Home directory.

10. Install Oracle SOA Suite under the same Middleware Home. Refer to Installing the Latest Version of Oracle SOA Suite (Oracle Identity Manager Users Only) for more information.

11. Run the `<IDM_Home>/common/bin/config.sh` script (on UNIX). (`<IDM_Home>\common\bin\config.cmd` on Windows). This IDM_Home is the directory where you installed Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Authorization Policy Manager, and Oracle Identity Navigator.

    The Oracle Fusion Middleware Configuration Wizard appears.

12. On the Welcome screen, select the **Extend an existing WebLogic domain** option. Click **Next**. The Select a WebLogic Domain Directory screen is displayed.

13. On the Select a WebLogic Domain Directory screen, select the Oracle Identity Management 11.1.1.3.0 domain in which you configured Oracle Internet Directory and Oracle Virtual Directory. Click **Next**. The Select Extension Source screen is displayed.

14. On the Select Extension Source screen, select the following domain configuration options:

■ **Oracle Identity Manager - 11.1.1.3.0 [Oracle_IDM1]**

> **Note:** When you select the **Oracle Identity Manager - 11.1.1.3.0 [Oracle_IDM1]** option, the following options are also selected, by default: **Oracle SOA Suite - 11.1.1.0 [Oracle_SOA1]**, and **Oracle WSM Policy Manager - 11.1.1.0 [oracle_common]**.

15. After selecting the domain configuration options, click **Next**. The Configure JDBC Component Schema screen is displayed.

16. On the Configure JDBC Component Schema screen, select a component schema, such as the SOA Infrastructure Schema, the User Messaging Service Schema, the OWSM MDS Schema, the OIM MDS Schema, the OIM Schema, or the SOA 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, the Select Optional Configuration screen appears.

17. On the Select Optional Configuration screen, you can configure **JMS Distributed Destination, Managed Servers, Clusters, and Machines**, **Deployments and Services**, and **JMS File Store**. Select the relevant check boxes and click **Next**.

■ Optional: Select a JMS Distributed Destination Type, as required.

■ Optional: Configure Managed Servers, as required.

■ Optional: Configure Clusters, as required. For more information about configuring clusters for Oracle Identity Management products, see the "Configuring High Availability for Identity Management Components" topic in the *Oracle Fusion Middleware High Availability Guide*.

■ Optional: Assign Managed Servers to Clusters, as required.

■ 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.

■ 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 JMS File Store, as required.

18. On the Configuration Summary screen, review the domain configuration, and click **Extend** to start extending the domain.

Your existing Oracle Identity Management 11.1.1.1.3.0 domain with Oracle Internet Directory and Oracle Virtual Directory is extended to support Oracle Identity Manager.

19. Start the Administration Server, as described in Starting the Stack.

20. Run the LDAP Preconfiguration Utility, as described in the "Task 1: Running the LDAP Preconfiguration Utility" topic in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

21. 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_11
```

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_11, 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**.

d. At the DOS command prompt, type the following command:

```
java -jar <MW_HOME>modules/com.bea.core.jarbuilder_
1.5.0.0.jar
```

This command generates the `wlfullclient.jar` file.

22. Configure Oracle Identity Manager Server, as described in Configuring OIM Server, Design Console, and Remote Manager. When configuring Oracle Identity Manager Server, ensure that you select the **Enable LDAP Sync** option on the LDAP Sync and OAM Screen in the Oracle Identity Manager Configuration Wizard.

23. Follow the wizard to complete the configuration.

24. Restart your Administration Server, and then start the SOA and OIM Managed Servers.

25. Run the LDAP Post-Configuration Utility, as described in the "Task 3: Running the LDAP Post-Configuration Utility" topic in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

26. Verify LDAP Synchronization, as described in the "Verifying LDAP Synchronization" topic in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

5.3.4 OIM with LDAP Sync, and OAM

This section discusses how to configure Oracle Identity Manager (OIM) and Oracle Access Manager (OAM) in different scenarios:

It includes the following sections:

- Overview
- Prerequisites
- Scenario 1: OIM with LDAP Sync, and OAM in a New WebLogic Domain
- Scenario 2: OIM with LDAP Sync, and OAM, in an Existing Domain Containing OID and OVD

5.3.4.1 Overview

In this section, you perform the following tasks:

1. Install and configure Oracle Internet Directory and Oracle Virtual Directory

2. Install and configure Oracle Identity Manager and Oracle Access Manager

3. Configure Oracle Access Manager to use Oracle Internet Directory as the LDAP provider

4. Set up LDAP sync for Oracle Identity Manager

5. Configure Oracle Identity Manager Server, Design Console (Windows only), and Remote Manager

5.3.4.2 Prerequisites

The following lists the prerequisites for installing and configuring Oracle Identity Manager with LDAP Synchronization, and Oracle Access Manager:

- Install a supported version of Oracle Database, as described in Installing Oracle Database.

- Create and load database schemas, as described in Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU).

- Install Oracle WebLogic Server 10.3.3 and creating a Middleware Home, as described in Installing Oracle WebLogic Server 10.3.3 and Creating the Oracle Middleware Home.

- Ensure that the Oracle Identity Management $11g$ Release 1 (11.1.1) suite containing Oracle Internet Directory (OID) and Oracle Virtual Directory (OVD) are installed, as described in Installing and Configuring OID, OVD, ODSM, ODIP, and OIF (11.1.1.4.0).

  An IDM_Home directory, such as **Oracle_IDM1**, is created. This directory is the Oracle Home for Oracle Internet Directory (OID), Oracle Virtual Directory (OVD), and Oracle Directory Services Manager (ODSM).

- Configure Oracle Internet Directory (OID) and Oracle Virtual Directory (OVD) in a WebLogic administration domain, as described in the "OID and OVD with ODSM in a New WebLogic Domain" topic in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

- Install Oracle Identity Management $11g$ Release 1 (11.1.1) suite containing Oracle Identity Manager (OIM), Oracle Access Manager (OAM) Oracle Adaptive Access Manager, Oracle Authorization Policy Manager (OAPM), and Oracle Identity Navigator (OIN), as described in Installing OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0).

  An IDM_Home directory, such as **Oracle_IDM2**, is created. This directory is the Oracle Home for Oracle Identity Manager (OIM) and Oracle Access Manager (OAM).

  > **Note:** It is assumed that you are installing and configuring Oracle Internet Directory (OVD), Oracle Virtual Directory (OVD), Oracle Identity Manager (OIM), and Oracle Access Manager (OAM) on the same machine. Therefore, two distinct IDM_Home directories are mentioned in this chapter.

- Install the latest version of Oracle SOA Suite under the same Middleware Home, and patch the Oracle SOA Suite to the latest version, as described in Installing the Latest Version of Oracle SOA Suite (Oracle Identity Manager Users Only).

5.3.4.3 Scenario 1: OIM with LDAP Sync, and OAM in a New WebLogic Domain

This section discusses the following topics:

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure

5.3.4.3.1 Appropriate Deployment Environment Perform the configuration in this topic if you want to install Oracle Identity Manager (OIM) with LDAP Synchronization in an environment where you may set up integration between Oracle Identity Manager and Oracle Access Manager (OAM) at a later time.

5.3.4.3.2 Components Deployed Performing the configuration in this section deploys the following:

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

5.3.4.3.3 Dependencies The configuration in this section depends on the following:

- Oracle WebLogic Server.
- Installation of the Oracle Identity Management 11*g* software.
- Installation and configuration of Oracle Internet Directory and Oracle Virtual Directory.
- Installation of the latest version of Oracle SOA Suite (required by Oracle Identity Manager).
- Database schemas for Oracle Identity Manager, Oracle SOA Suite, and Oracle Access Manager. For more information, see Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU).

5.3.4.3.4 Procedure Perform the following steps to configure Oracle Identity Manager with LDAP Synchronization, and Oracle Access Manager in a new WebLogic domain:

1. After completing all the prerequisites, run the `<Oracle_IDM2>/common/bin/config.sh` script on UNIX (`<Oracle_IDM2>\common\bin\config.cmd` on Windows). This Oracle_IDM2 is the directory where you installed Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Authorization Policy Manager, and Oracle Identity Navigator.

   The Oracle 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 is displayed.

3. On the Select Domain Source screen, select the following domain configuration options:

   - **Oracle Identity Manager - 11.1.1.3.0 [Oracle_IDM2]**

> **Note:** When you select the **Oracle Identity Manager - 11.1.1.3.0 [Oracle_IDM2]** option, the following options are also selected, by default: **Oracle SOA Suite - 11.1.1.0 [Oracle_SOA1]**, **Oracle Enterprise Manager - 11.1.1.0 [oracle_common]**, and **Oracle WSM Policy Manager - 11.1.1.0 [oracle_common]**.

- **Oracle Access Manager with Database Policy Store - 11.1.1.3.0 [Oracle_ IDM2]**

4. After selecting the domain configuration options, click **Next**. The Specify Domain Name and Location screen is displayed.

5. On the Specify Domain Name and Location screen, enter a name and location for the domain to be created. In addition, enter a location to store applications for the domain. Click **Next**. The Configure Administrator User Name and Password screen is displayed.

6. 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 is displayed.

7. Choose JRockit SDK 1.6.0_17 and Production Mode in the Configure Server Start Mode and JDK screen of the Oracle Fusion Middleware Configuration Wizard. Click **Next**. Tthe Configure JDBC Component Schema screen is displayed.

8. On the Configure JDBC Component Schema screen, select a component schema, such as the OAM Infrastructure Schema, the SOA Infrastructure Schema, the User Messaging Service Schema, the OWSM MDS Schema, the OIM MDS Schema, the OIM Schema, or the SOA 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, the Select Optional Configuration screen appears.

9. On the Select Optional Configuration screen, you can configure **Administration Server, Managed Servers, Clusters, and Machines**, **Deployments and Services**, **RDBMS Security Store**, and **JMS File Store**. Select the relevant check boxes and click **Next**.

   - Optional: Configure Administration Server, as required.

   - Optional: Configure Managed Servers, as required.

   - Optional: Configure Clusters, as required.

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

   - Optional: Assign Managed Servers to Clusters, as required.

   - 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, as required.

- Optional: Configure JMS File Store, as required.

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 Identity Manager and 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.

11. Start the WebLogic Administration Server and Managed Servers (Oracle Identity Manager and Oracle Access Manager), as described in Starting the Stack.

12. Configure Oracle Access Manager (OAM) to use Oracle Internet Directory (OID) as an LDAP provider by running the `createUserIdentityStore` WLST command:

    a. On the command line, use the cd command to move from your present working directory to the `Oracle_IDM2/common/bin` directory. **Oracle_IDM2** is the IDM_Home for Oracle Identity Manager and Oracle Access Manager.

    b. 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*.

    Run the `createUserIdentityStore` WLST command, as in the following example:

    ```
    createUserIdentityStore(name="OAMOIDIdStoreForOIM",princip
    al="cn=orcladmin", credential="welcome1", type="LDAP",
    userAttr="uid", ldapProvider="OID",
    roleSecAdmin="OAMAdministrators",
    userSearchBase="cn=Users,dc=us,dc=acme,dc=com"
    ,ldapUrl="ldap://<oid host>:<oid port>" ,isPrimary="true"
    ,userIDProvider="OracleUserRoleAPI" ,
    groupSearchBase="cn=Groups,dc=us,dc=acme,dc=com")
    ```

> **Note:** Users that are members of the group specified in the
> `roleSecAdmin` attribute are allowed access to the Oracle Access
> Manager Administration Console. This group must exist under the
> Directory Information Tree (DIT) specified in the `groupSearchBase`
> attribute. If the group is not available, you can specify the user name,
> such as `orcladmin`, who will have access to the Oracle Access
> Manager Administration Console. Note that only the user specified in
> this attribute will have access to the Oracle Access Manager
> Administration Console.

Alternatively, you can use the Oracle Access Manager Administration Console,
deployed on the Administration Server, to configure Oracle Internet Directory as
an LDAP provider for Oracle Access Manager. For more information, see the
"Managing User-Identity Store and OAM Administrator Registrations" topic in the
guide *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager*.

13. Set up LDAP Synchronization, as described in the "Setting Up LDAP
    Synchronization" topic in the *Oracle Fusion Middleware Installation Guide for Oracle
    Identity Management*.

14. Verify LDAP Synchronization, as described in the "Verifying LDAP
    Synchronization" topic in the *Oracle Fusion Middleware Installation Guide for Oracle
    Identity Management*.

15. Configure Oracle Identity Manager Server, as described in Configuring OIM
    Server. When configuring Oracle Identity Manager Server, ensure that you select
    the **Enable LDAP Sync** option on the LDAP Sync and OAM Screen in the Oracle
    Identity Manager Configuration Wizard.

16. Follow the wizard and the steps described in Configuring OIM Server to complete
    the Oracle Identity Manager Server configuration. Similarly, follow the wizard to
    configure Oracle Identity Manager Design Console (Windows only) and to
    configure Oracle Identity Manager Remote Server, as described in Configuring
    OIM Design Console, and Configuring OIM Remote Manager.

5.3.4.4 Scenario 2: OIM with LDAP Sync, and OAM, in an Existing Domain Containing OID and OVD

This section discusses the following topics:

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure

5.3.4.4.1 Appropriate Deployment Environment Perform the configuration in this topic if
you want to install Oracle Identity Manager (OIM) with LDAP Synchronization in an
environment where you have installed and configured Oracle Internet Directory (OID)
and Oracle Virtual Directory (OVD). At a later time, you may set up integration
between Oracle Identity Manager and Oracle Access Manager (OAM) at a later time.

5.3.4.4.2 Components Deployed Performing the configuration in this section deploys the
following:

- Managed Servers for Oracle Identity Manager and Oracle Access 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

- Oracle Access Manager Console on the existing Administration Server

5.3.4.4.3 Dependencies The configuration in this section depends on the following:

- Oracle WebLogic Server.

- Installation and configuration of Oracle Internet Directory and Oracle Virtual Directory.

- Installation of the Oracle Identity Management 11*g* software.

- Installation of the latest version of Oracle SOA Suite (required by Oracle Identity Manager).

- Database schemas for Oracle Identity Manager, Oracle SOA Suite, and Oracle Access Manager. For more information, see Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU).

5.3.4.4.4 Procedure Perform the following steps to configure Oracle Identity Manager with LDAP Synchronization, and Oracle Access Manager in an existing Oracle Identity Management 11.1.1.3.0 domain that contains Oracle Internet Directory and Oracle Virtual Directory:

1. After completing the prerequisites, run the `<Oracle_IDM1>/bin/config.sh` on UNIX operating systems to start the Oracle Identity Management Configuration Wizard. On Windows, run the `<Oracle_IDM1>\bin\config.bat` to start the wizard. The Oracle_IDM1 home is the directory where you installed Oracle Internet Directory, Oracle Virtual Directory, Oracle Directory Services Manager, Oracle Directory Integration Platform, and Oracle Identity Federation.

2. On the Select Domain screen, select the **Create New Domain** option. Set the Administrator user name and password, as required.

3. Ensure that you select **Oracle Internet Directory** and **Oracle Virtual Directory** on the Configure Components screen.

4. Follow the wizard, provide the necessary input, and configure the domain.

   A new WebLogic domain to support Oracle Internet Directory and Oracle Virtual Directory 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.

5. Ensure that your Oracle database version is supported and you have installed the necessary patches. For more information, see Installing Oracle Database.

6. Ensure that any appropriate schemas required by Oracle Identity Manager, Oracle SOA Suite, and Oracle Access Manager are created and loaded, as described in Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU).

7. Ensure that the Oracle Identity Management 11*g* software is installed. Refer to Installing OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0) for more information. A new Oracle Home for Oracle Identity Management, such as `Oracle_IDM2`, is created under the Middleware Home directory.

8. Ensure that the latest version of Oracle SOA Suite is installed under the same Middleware Home. Refer to Installing the Latest Version of Oracle SOA Suite (Oracle Identity Manager Users Only) for more information.

9. Run the `<Oracle_IDM2>/common/bin/config.sh` script (on UNIX). (`<Oracle_IDM2>\common\bin\config.cmd` on Windows). The Oracle Fusion Middleware Configuration Wizard appears.

10. On the Welcome screen, select the **Extend an existing WebLogic domain** option. Click **Next**. The Select a WebLogic Domain Directory screen is displayed.

11. On the Select a WebLogic Domain Directory screen, select the Oracle Identity Management 11.1.1.3.0 domain in which you configured Oracle Internet Directory and Oracle Virtual Directory. Click **Next**. The Select Extension Source screen is displayed.

12. On the Select Extension Source screen, select the following domain configuration options:

    ■ **Oracle Identity Manager - 11.1.1.3.0 [Oracle_IDM2]**

    Note: When you select the **Oracle Identity Manager - 11.1.1.3.0 [Oracle_IDM2]** option, the following options are also selected, by default: **Oracle SOA Suite - 11.1.1.0 [Oracle_SOA1]**, and **Oracle WSM Policy Manager - 11.1.1.0 [oracle_common]**.

    ■ **Oracle Access Manager with Database Policy Store - 11.1.1.3.0 [Oracle_IDM2]**

13. After selecting the domain configuration options, click **Next**. The Configure JDBC Component Schema screen is displayed.

14. On the Configure JDBC Component Schema screen, select a component schema, such as the OAM Infrastructure Schema, the SOA Infrastructure Schema, the User Messaging Service Schema, the OWSM MDS Schema, the OIM MDS Schema, the OIM Schema, or the SOA 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, the Select Optional Configuration screen appears.

15. On the Select Optional Configuration screen, you can configure **JMS Distributed Destination, Managed Servers, Clusters, and Machines**, **Deployments and Services**, and **JMS File Store**. Select the relevant check boxes and click **Next**.

    ■ Optional: Select a JMS Distributed Destination Type, as required.

    ■ Optional: Configure Managed Servers, as required.

    ■ Optional: Configure Clusters, as required.

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

    ■ Optional: Assign Managed Servers to Clusters, as required.

    ■ 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 JMS File Store, as required.

16. On the Configuration Summary screen, review the domain configuration, and click **Extend** to start extending the domain.

    Your existing Oracle Identity Management 11.1.1.1.3.0 domain with Oracle Internet Directory and Oracle Virtual Directory is extended to support Oracle Identity Manager and Oracle Access Manager.

17. Start the WebLogic Administration Server and Managed Servers (Oracle Identity Manager and Oracle Access Manager), as described in Starting the Stack.

18. Configure Oracle Access Manager (OAM) to use Oracle Internet Directory (OID) as an LDAP provider by running the `createUserIdentityStore` WLST command:

    a. On the command line, use the cd command to move from your present working directory to the `Oracle_IDM2/common/bin` directory. **Oracle_IDM2** is the IDM_Home for Oracle Identity Manager and Oracle Access Manager.

    b. 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*.

    Run the `createUserIdentityStore` WLST command, as in the following example:

    ```
    createUserIdentityStore(name="OAMOIDIdStoreForOIM",princip
    al="cn=orcladmin", credential="welcome1", type="LDAP",
    userAttr="uid", ldapProvider="OID",
    roleSecAdmin="OAMAdministrators",
    userSearchBase="cn=Users,dc=us,dc=acme,dc=com"
    ,ldapUrl="ldap://<oid host>:<oid port>" ,isPrimary="true"
    ,userIDProvider="OracleUserRoleAPI" ,
    groupSearchBase="cn=Groups,dc=us,dc=acme,dc=com")
    ```

> **Note:** Users that are members of the group specified in the `roleSecAdmin` attribute are allowed access to the Oracle Access Manager Administration Console. This group must exist under the Directory Information Tree (DIT) specified in the `groupSearchBase` attribute. If the group is not available, you can specify the user name, such as `orcladmin`, who will have access to the Oracle Access Manager Administration Console. Note that only the user specified in this attribute will have access to the Oracle Access Manager Administration Console.

Alternatively, you can use the Oracle Access Manager Administration Console, deployed on the Administration Server, to configure Oracle Internet Directory as an LDAP provider for Oracle Access Manager. For more information, see the "Managing User-Identity Store and OAM Administrator Registrations" topic in the guide *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager*.

19. Set up LDAP Synchronization, as described in the "Setting Up LDAP Synchronization" topic in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

20. Verify LDAP Synchronization, as described in the "Verifying LDAP Synchronization" topic in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

21. Configure Oracle Identity Manager Server, as described in Configuring OIM Server. When configuring Oracle Identity Manager Server, ensure that you select the **Enable LDAP Sync** option on the LDAP Sync and OAM Screen in the Oracle Identity Manager Configuration Wizard.

22. Follow the wizard and the steps described in Configuring OIM Server to complete the Oracle Identity Manager Server configuration. Similarly, follow the wizard to configure Oracle Identity Manager Design Console (Windows only) and to configure Oracle Identity Manager Remote Server, as described in Configuring OIM Design Console, and Configuring OIM Remote Manager.

5.3.5 OAM in a New WebLogic Domain

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

It includes the following sections:

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure

5.3.5.1 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 Management components, such as Oracle Identity Navigator, Oracle Identity Manager, and Oracle Adaptive Access Manager at a later time in the same domain.

5.3.5.2 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

5.3.5.3 Dependencies

The configuration in this section depends on the following:

- Oracle WebLogic Server

- Installation of the Oracle Identity Management 11*g* software

- Database schemas for Oracle Access Manager.

5.3.5.4 Procedure

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

1. Install Oracle WebLogic Server and create a Middleware Home. Refer to Installing Oracle WebLogic Server 10.3.3 and Creating the Oracle Middleware Home for more information.

2. Create and load the appropriate schemas required by Oracle Access Manager, as described in Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU).

3. Install the Oracle Identity Management 11*g* software. Refer to Installing OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0) for more information.

4. Run the `<IDM_Home>/common/bin/config.sh` script (on UNIX). (`<IDM_Home>\common\bin\config.cmd` on Windows). This IDM_Home is the directory where you installed Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Authorization Policy Manager, and Oracle Identity Navigator.

   The Oracle Fusion Middleware Configuration Wizard appears.

5. On the Welcome screen, select the **Create a new WebLogic domain** option. Click **Next**. The Select Domain Source screen appears.

6. 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**, 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** option, the **Oracle JRF 11.1.1.0 [Oracle_Common]** option is also selected, by default.

7. Enter a name and a location for the domain to be created, and click **Next**. The Configure Administrator User Name and Password screen appears.

8. Configure a user name and a password for the administrator. The default user name is `weblogic`. Click **Next**.

9. Choose `JRockit SDK 1.6.0_17` and Production Mode in the Configure Server Start Mode and JDK screen of the Oracle Fusion Middleware Configuration Wizard. Click **Next**. The Select Optional Configuration screen appears.

10. On the Select Optional Configuration screen, you can configure the **Administration Server** and **Managed Servers, Clusters, and Machines**. Click **Next**.

11. Optional: Configure the following Administration Server parameters:

    - Name

    - Listen address

    - Listen port

    - SSL listen port

    - SSL enabled or disabled

12. 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.

13. Optional: Configure Clusters, as required. For more information about configuring clusters for Oracle Identity 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.

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.

16. Optional: 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.

17. Optional: Assign the newly created Managed Server, such as `oam_server1`, to a machine.

18. 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.

5.3.6 OAAM in a New WebLogic Domain

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

- Appropriate Deployment Environment

- Components Deployed

- Dependencies

- [Procedure](#)

5.3.6.1 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 Management 11*g* components, such as Oracle Identity Navigator, Oracle Access Manager, or Oracle Identity Manager at a later time in the same domain.

5.3.6.2 Components Deployed

Performing the configuration in this section deploys the following:

- WebLogic Administration Server

- Managed Server for Oracle Adaptive Access Manager

- Oracle Adaptive Access Manager Console on the Administration Server

5.3.6.3 Dependencies

The configuration in this section depends on the following:

- Oracle WebLogic Server

- Installation of the Oracle Identity Management 11*g* software

- Database schema for Oracle Adaptive Access Manager

5.3.6.4 Procedure

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

1. Install Oracle WebLogic Server and create a Middleware Home, as described in [Installing Oracle WebLogic Server 10.3.3 and Creating the Oracle Middleware Home](#).

2. Create and load the appropriate schemas required by Oracle Adaptive Access Manager, as described in [Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU)](#).

3. Install the Oracle Identity Management 11*g* software under your Middleware Home, as described in [Installing OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0)](#).

4. Run the `<IDM_Home>/common/bin/config.sh` script (on UNIX). (`<IDM_Home>\common\bin\config.cmd` on Windows). This IDM_Home is the directory where you installed Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Authorization Policy Manager, and Oracle Identity Navigator.

   The Oracle Fusion Middleware Configuration Wizard appears.

5. On the Welcome screen, select the **Create a new WebLogic domain** option. Click **Next**. The Select Domain Source screen appears.

6. 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**, which is mandatory.

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

> **Note:** When you select either of the Oracle Adaptive Access
> Manager options, the **Oracle JRF - 11.1.1.0 [oracle_common]** option,
> the **Oracle Identity Navigator - 11.1.1.3.0 [Oracle_IDM1]** option, and
> the **Oracle WSM Policy Manager - 11.1.1.0 [Oracle_IDM1]** option are
> also selected, by default.

7. Enter a name and a location for the domain to be created, and click **Next**. The
   Configure Administrator User Name and Password screen appears.

8. Configure a user name and a password for the administrator. The default user
   name is `weblogic`. Click **Next**.

9. Choose `JRockit SDK 1.6.0_17` and Production Mode in the Configure Server
   Start Mode and JDK screen of the Oracle Fusion Middleware Configuration
   Wizard.

10. On the Configure JDBC Data Sources screen, select the `OAAM_ADMIN_DS` data
    source for the Oracle Adaptive Access Manager Server application. If you selected
    the Oracle Adaptive Access Manager - Server - 11.1.1.3.0 option on the Select
    Domain source screen, you can also select the OAAM_SERVER_DS data source.
    Configure default database credentials, such as Schema Name, Password,
    Database Service Name, Host Name, and Port. Click **Next**.

    The Test JDBC Data Sources screen appears. After the test succeeds, the Select
    Optional Configuration screen appears.

11. On the Select Optional Configuration screen, you can configure the
    Administration Server and **Managed Servers, Clusters, and Machines**, and
    Deployments and Services. Click **Next**.

12. Optional: Configure the following Administration Server parameters:

    - Name

    - Listen address

    - Listen port

    - SSL listen port

    - SSL enabled or disabled

13. Optional: Configure Managed Servers, as required.

14. Optional: Configure Clusters, as required. For more information about configuring
    clusters for Oracle Identity Management products, see the "Configuring High
    Availability for Identity Management Components" topic in the guide *Oracle
    Fusion Middleware High Availability Guide*.

15. Optional: Assign Managed Servers to Clusters, as required.

16. 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.

17. Optional: Assign the Administration Server to a machine.

18. Optional: Select Deployments, such as applications and libraries, and Services to
    target them to a particular cluster or server.

19. 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.

5.3.7 OAPM in a New WebLogic Domain

This topic describes how to configure Oracle Authorization Policy Manager (OAPM) in a new WebLogic domain. It includes the following sections:

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure

5.3.7.1 Appropriate Deployment Environment

Perform the configuration in this topic if you want to install Oracle Authorization Policy Manager in an environment where you may install Oracle Identity Manager, Oracle Access Manager, Oracle Identity Management Navigator, or Oracle Adaptive Access Manager at a later stage in the same domain.

5.3.7.2 Components Deployed

Performing the configuration in this section deploys the following:

- WebLogic Administration Server
- Oracle Authorization Policy Manager application on the Administration Server

5.3.7.3 Dependencies

The configuration in this section depends on the following:

- Oracle WebLogic Server.
- Installation of the Oracle Identity Management 11*g* software.
- Database schema for Oracle Authorization Policy Manager and Metadata Services (MDS).

5.3.7.4 Procedure

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

1. Install Oracle WebLogic Server and create a Middleware Home, as described in Installing Oracle WebLogic Server 10.3.3 and Creating the Oracle Middleware Home.

2. Create and load the database schemas for Oracle Authorization Policy Manager, as described in Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU).

3. Install the Oracle Identity Management 11*g* software under your Middleware Home. Refer to Installing OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0) for more information.

4. Run the `<IDM_Home>/common/bin/config.sh` script (on UNIX). (`<IDM_Home>\common\bin\config.cmd` on Windows). This IDM_Home is the directory where you installed Oracle Identity Manager, Oracle Access Manager,

Oracle Adaptive Access Manager, Oracle Authorization Policy Manager, and Oracle Identity Navigator.

The Oracle Fusion Middleware Configuration Wizard appears.

5. On the Welcome screen, select the **Create a new WebLogic domain** option. Click **Next**. The Select Domain Source screen appears.

6. 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 Application Authorization Policy Manager - 11.1.1.3.0** option.

   When you select this option, the **Oracle JRF 11.1.1.0 [oracle_common]** option is also selected, by default. For association with Oracle Enterprise Manager Fusion Middleware Control at a later stage, select the **Oracle Enterprise Manager - 11.1.1.3.0 [oracle_common]** template. Click **Next**. The Select Domain Name and Location screen appears.

7. Enter a name and a location for the domain to be created, and click **Next**. The Configure Administrator User Name and Password screen appears.

8. Configure a user name and a password for the administrator. The default user name is `weblogic`. Click **Next**.

9. Choose `JRockit SDK 1.6.0_17` and Production Mode in the Configure Server Start Mode and JDK screen of the Oracle Fusion Middleware Configuration Wizard. Click **Next**. The Configure JDBC Component Schema screen is displayed.

10. On the Configure JDBC Component Schema screen, select a component schema, such as the APM MDS Schema or the APM 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.

11. 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 Authorization Policy Manager 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 Management products, see the "Configuring High Availability for Identity Management Components" topic in the guide *Oracle Fusion Middleware High Availability Guide*.

    - Optional: Assign Managed Servers to Clusters, as required.

- 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.

- 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.

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

A new WebLogic domain to support Oracle Authorization Policy 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.

5.3.8 OAPM in a Domain Containing OIM, OAM, OAAM, and OIN

This topic describes how to configure Oracle Authorization Policy Manager (OAPM) in an existing Oracle Identity Management domain that contains Oracle Identity Manager (OIM), Oracle Access Manager (OAM), Oracle Adaptive Access Manager (OAAM), and Oracle Identity Navigator (OIN).

It includes the following sections:

- Appropriate Deployment Environment

- Components Deployed

- Dependencies

- Procedure

5.3.8.1 Appropriate Deployment Environment

Perform the configuration in this topic if you want to install Oracle Authorization Policy Manager in an environment where Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Navigator are installed and configured.

5.3.8.2 Components Deployed

Performing the configuration in this section deploys the Oracle Authorization Policy Manager application on the existing WebLogic Administration Server.

5.3.8.3 Dependencies

The configuration in this section depends on the following:

- Oracle WebLogic Server.

- Installation of the Oracle Identity Management 11*g* software.

- Installation of the latest version of Oracle SOA Suite (required by Oracle Identity Manager.

- Database schema for Oracle Authorization Policy Manager and Metadata Services (MDS) schema.

5.3.8.4 Procedure

To configure Oracle Authorization Policy Manager in an existing WebLogic domain that contains Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Management Navigator, complete the following steps:

1. Install Oracle WebLogic Server and create a Middleware Home, as described in Installing Oracle WebLogic Server 10.3.3 and Creating the Oracle Middleware Home.

2. Create and load the schemas for Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Authorization Policy Manager by using Oracle Fusion Middleware Repository Creation Utility (RCU), as described in Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU).

3. Install the Oracle Identity Management 11*g* software under your Middleware Home. Refer to Installing OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0) for more information.

4. Run the `<IDM_Home>/common/bin/config.sh` script (on UNIX). (`<IDM_Home>\common\bin\config.cmd` on Windows). This IDM_Home is the directory where you installed Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Authorization Policy Manager, and Oracle Identity Navigator.

    The Oracle Fusion Middleware Configuration Wizard appears.

5. Create a new WebLogic domain to support Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Management Navigator.

    For more information, see the "Simultaneous configuration of OIN, OAPM, OAAM, OAM, and OIM" topic in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

    > **Note:** On the Select Domain Source screen, do not select the **Oracle Authorization Policy Manager - 11.1.1.3.0 [Oracle_IDM1]** option.

6. Ensure that the WebLogic domain with Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Management Navigator is configured correctly.

    After the domain configuration is complete, click **Done** to dismiss the Oracle Fusion Middleware Configuration Wizard.

    A new WebLogic domain to support Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, and 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.

7. Run the `<IDM_Home>/common/bin/config.sh` script (on UNIX). (`<IDM_Home>\common\bin\config.cmd` on Windows). This IDM_Home is the directory where you installed Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Authorization Policy Manager, and Oracle Identity Navigator.

    The Oracle Fusion Middleware Configuration Wizard appears.

8. On the Welcome screen, select the **Extend an existing WebLogic domain** option. Click **Next**.

9. On the Select a WebLogic Domain Directory screen, browse to the `<MW_HOME>/user_projects/domains` directory where you created the domain with Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Navigator. Click **Next**.

    The Select Extension Source screen appears.

10. On the Select Extension Source screen, ensure that the **Extend my domain automatically to support the following products:** option is selected. Select **Oracle Application Authorization Policy Manager - 11.1.1.3.0**. Click **Next**. The Configure JDBC Component Schema screen appears.

11. On the Configure JDBC Component Schema screen, select a component schema that you want to modify.

    The screen lists the following component schemas:

    ■   SOA Infrastructure

    ■   OAAM Admin Schema

    ■   OAAM Server Schema

    ■   User Messaging Service

    ■   APM MDS Schema

    ■   APM Schema

    ■   OAAM Admin MDS Schema

    ■   OIM MDS Schema

    ■   OWSM MDS Schema

    ■   SOA MDS Schema

    ■   OIM Schema

    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.

12. On the Select Optional Configuration screen, you can configure **Managed Servers, Clusters, and Machines**, **Deployments and Services**, and **JMS File Store**. Select the relevant check boxes, and Click **Next**.

    ■   Optional: Configure Managed Servers, as required.

    ■   Optional: Configure Clusters, as required. For more information about configuring clusters for Oracle Identity Management products, see the "Configuring High Availability for Identity Management Components" topic in the guide *Oracle Fusion Middleware High Availability Guide*.

    ■   Optional: Assign Managed Servers to Clusters, as required.

    ■   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.

    ■   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, such as oam_server1 (default value).

- Optional: Configure JMS File Stores, as required.

13. On the Configuration Summary screen, review the domain configuration, and click **Extend** to start extending the existing domain, which contains Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Navigator, to support Oracle Authorization Policy Manager.

5.4 Configuring OIM Server, Design Console, and Remote Manager

After configuring Oracle Identity Manager (OIM) in a new or existing WebLogic administration domain, you must run the Oracle Identity Manager 11*g* Configuration Wizard to configure the following:

- Oracle Identity Manager Server

- Oracle Identity Manager Design Console (on Windows operating systems only)

- Oracle Identity Manager Remote Manager

> **Note:** For information about configuring Oracle Identity Manager Server, Design Console, and Remote Manager after configuring Oracle Identity Manager in a new or existing WebLogic domain, see Chapter 6, "Configuring OIM Server, Design Console, and Remote Manager".

5.5 Oracle Identity Management Suite-Level Installation Scenarios

For information about Oracle Identity Management suite-level installation scenarios, see the chapter "Oracle Identity Management Suite-Level Installation Scenarios" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

5.6 Installing Oracle HTTP Server 11*g* WebGate for OAM

For information about installing and configuring Oracle HTTP Server 11*g* WebGate for Oracle Access Manager (OAM), see the chapter "Installing and Configuring Oracle HTTP Server 11g WebGate for OAM" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

5.7 Setting Up Integration Between OIM and OAM

For information about setting up integration between Oracle Identity Manager (OIM) and Oracle Access Manager (OAM), see the chapter "Integration Between OIM and OAM" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

6

Configuring OIM Server, Design Console, and Remote Manager

This chapter explains how to configure Oracle Identity Manager (OIM) Server, Design Console, and Remote Manager after configuring the Oracle Identity Manager application in a new or existing WebLogic domain.

It includes the following topics:

- Configuring OIM Server, Design Console, and Remote Manager
- Before Configuring OIM Server, Design Console, or Remote Manager
- Starting the Oracle Identity Manager 11g Configuration Wizard
- Configuring OIM Server
- Installing and Configuring Only OIM Design Console on Windows
- Configuring OIM Design Console
- Configuring OIM Remote Manager

Note: The Oracle Identity Manager Configuration Wizard enables you to configure only some fundamental non-J2EE elements of Oracle Identity Manager, such as Oracle Identity Manager Server, Oracle Identity Manager Design Console, and Oracle Identity Manager Remote Manager. For more information about configuring and administering Oracle Identity Manager, see the *Oracle Identity Manager System Administrator's Guide*.

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.

6.1 Configuring OIM Server, Design Console, and Remote Manager

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

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, Design Console, or Remote Manager 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.

Note that Oracle Identity Manager requires Oracle SOA Suite 11*g* (11.1.1.3.0), which should be exclusive to Oracle Identity 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.

6.2 Before Configuring OIM Server, Design Console, or Remote Manager

Before configuring Oracle Identity Manager (OIM) using the Oracle Identity Manager Wizard, ensure that you have completed the prerequisites for configuring Oracle Identity Manager components (Server, Design Console, and Remote Manager).

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

6.2.1 Prerequisites for Configuring OIM Server

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

1. Installing Oracle WebLogic Server 10.3.3 and created a Middleware Home directory. For more information, see Installing Oracle WebLogic Server 10.3.3 and Creating the Oracle Middleware Home.

2. Installing a supported version of Oracle database. For more information, see Installing Oracle Database.

3. Creating and loading the required schemas (OIM and MDS) in the database. For more information, see Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU).

4. Installing the Oracle Identity Management Suite (the suite that contains Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Authorization Policy Manager, and Oracle Identity Navigator) under the Middleware Home directory. For more information, see Installing OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0).

5. Installing Oracle SOA Suite 11*g* Release 1(11.1.1.3.0) under the same Middleware Home directory. For more information, see Installing the Latest Version of Oracle SOA Suite (Oracle Identity Manager Users Only).

6. Configuring Oracle Identity Manager and Oracle SOA Suite in the same WebLogic administration domain (a new or existing domain). For more information, see the example scenarios described in Basic Installation and Configuration Scenarios.

7. Starting the Oracle WebLogic Administration Server for the domain in which the Oracle Identity Manager application is deployed. For more information, see Starting the Stack.

8. Optional: Setting up LDAP Synchronization for Oracle Identity Manager, if you want to enable LDAP Sync. For more information, see the topic "Setting Up LDAP Synchronization" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

9. Optional: Installing Oracle BI Publisher, if you want to configure Oracle BI Publisher for reporting features in Oracle Identity Manager. For more information, see the guide *Oracle Fusion Middleware Quick Installation Guide for Oracle Business Intelligence*.

6.2.2 Prerequisites for Configuring Only OIM Design Console on a Different Machine

On the machine where you are installing and configuring Design Console, you must install the Oracle Identity Management 11*g* (11.1.1.3.0) software containing Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Authorization Policy Manager, and Oracle Identity Navigator. For information, see Installing OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0).

Before you can configure Oracle Identity Manager (OIM) Design Console by running the Oracle Identity Manager Configuration Wizard, you should have configured the Oracle Identity Manager Server, as described in Configuring OIM Server on a local or 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 Management software.

6.2.3 Prerequisites for Configuring Only OIM Remote Manager on a Different Machine

On the machine where you are installing and configuring Remote Manager, you must install the Oracle Identity Management 11*g* (11.1.1.3.0) software containing Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Authorization Policy Manager, and Oracle Identity Navigator. For information, see Installing OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0).

Before you can configure Oracle Identity Manager (OIM) Remote Manager by running the Oracle Identity Manager Configuration Wizard, you should have configured the Oracle Identity Manager Server, as described in Configuring OIM 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 Management software.

6.3 Starting the Oracle Identity Manager 11*g* Configuration Wizard

To start the Oracle Identity Manager 11*g* Configuration Wizard, execute the `<IDM_Home>/bin/config.sh` script (on UNIX) on the machine where the Administration Server is running. (`<IDM_Home>\bin\config.bat` on Windows). This IDM_Home is the directory where you installed Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Authorization Policy Manager, and Oracle Identity Navigator.

The Oracle Identity Management 11*g* Configuration Wizard starts, and the Welcome Screen appears.

6.4 Configuring OIM Server

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

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure
- Post-Configuration Steps

6.4.1 Appropriate Deployment Environment

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

6.4.2 Components Deployed

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

6.4.3 Dependencies

The installation and configuration in this section depends on Oracle WebLogic Server, on Oracle SOA Suite, and on the installation of Oracle Identity Management 11*g* software. For more information, see Before Installing OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0) and Installing OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0).

6.4.4 Procedure

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

1. Ensure that all the prerequisites, described in Prerequisites for Configuring OIM Server, are satisfied.

> **Note:** If you extended an existing WebLogic domain to support
> Oracle Identity Manager, restart the Administration Server before
> starting the Oracle Identity Manager Configuration Wizard.

2. On the machine where the Administration Server is running, start the Oracle
   Identity Manager Configuration Wizard, as described in 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 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
   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 (OIM) 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 (OIM) 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 LDAP Sync and OAM screen appears.

    The LDAP Sync and OAM screen enables you to perform the following optional tasks:

    - Enable synchronization of Oracle Identity Manager roles, users, and their hierarchy to an LDAP directory

    - Enable Identity Administration Integration with Oracle Access Manager (OAM)

    - Configure Oracle Identity Manager to use Oracle BI Publisher for reporting purposes

15. Optional: To enable LDAP Sync, you must select the **Enable LDAP Sync** option on the LDAP Sync and OAM screen. However, note that you must first set up LDAP Sync for Oracle Identity Manager (OIM), as described in the topic "Setting Up LDAP Synchronization" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*, before enabling LDAP Sync.

16. Optional: To enable identity administration integration with Oracle Access Manager, select the **Enable Identity Administration Integration with OAM** option on the LDAP Sync and OAM screen, and enter the following information:

- **Password of Access Gate** - Enter the access gate password for Oracle Identity Manager. You must specify the same `oimAccessGatePwd` password that you provided when running the `configureOIM` WLST command. For more information about this WLST command and the complete setup to integrate OIM and OAM, see the topic "Setting Up Integration Between OIM and OAM Using the Domain Agent" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

- **Domain of Cookie** - Enter the domain of the machine on which Oracle HTTP Server for Oracle Identity Manager is running. You must specify the same `oimCookieDomain` value that you provided when running the `configureOIM` WLST command.

> **Note:** When you choose to enable identity administration integration with Oracle Access Manager, LDAP Synchronization is enabled, by default.

---

17. Optional: To configure Oracle Identity Manager to use Oracle BI Publisher for reporting purposes, select the **Configure BI Publisher** option, and enter the **BI Publisher URL** in the **BI Publisher URL** field. Note that you should have installed Oracle BI Publisher on a local or remote machine before selecting the **Configure BI Publisher** option on the LDAP Sync and OAM screen. In addition, ensure that Oracle BI Publisher is up and running.

18. After making your selections, click **Next** on the LDAP Sync and OAM screen. If you chose to enable identity administration integration with OAM or enable LDAP Sync, the LDAP Server screen appears.

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

    - **LDAP URL** - enter the LDAP URL in the format: `ldap://ovd_host:ovd_port`

    - **LDAP User** - enter the LDAP user name.

    - **LDAP Password** - enter the LDAP password.

    - **LDAP SearchDN** - enter the Distinguished Names (DN). For example, dc=acme, dc=com. SearchDN 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.

19. 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`.

> **Note:** For more information about user reservation containers in Oracle Internet Directory, see the guide *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*.

After enabling LDAP synchronization, you can verify it by using the Oracle Identity Manager Administration Console. Click **Next**. The Configuration Summary screen appears.

20. If you did not choose the **Enable LDAP Sync** option or the **Enable Identity Administration Integration with OAM** option on the LDAP Sync and OAM 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 the topic "Performing Silent Installations" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

    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 Locating 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.

21. Click **Finish**.

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

6.4.5 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: Edit the `<IDM_Home>\server\bin\setenv.bat` file in a text editor, and set the path of the *XEL_HOME* variable to the absolute path of `<IDM_Home>\server`. For example, if your IDM_Home is the `C:\oracle\Middleware\Oracle_IDM1` directory, then set *XEL_HOME* in the `setenv.bat` file to the `C:\oracle\Middleware\Oracle_IDM1\server` directory.

    On UNIX: Edit the `<IDM_Home>/server/bin/setenv.sh` file in a text editor, and set the path of the *XEL_HOME* variable to the absolute path of `<IDM_Home>/server`. For example, if your IDM_Home is the `/test/Middleware/Oracle_IDM1` directory, then set *XEL_HOME* in the `setenv.sh` file to the `/test/Middleware/Oracle_IDM1/server` directory.

- After installing and configuring Oracle Identity Manager Server for the first time, you must start the Oracle Identity Manager Managed Server. For information about starting the server, see Starting the Stack.

6.5 Installing and Configuring Only OIM Design Console on Windows

Table 6–1 lists the steps required to install and configure only Oracle Identity Manager (OIM) Design Console on Windows operating systems.

Table 6–1   Design Console Installation and Configuration Workflow

Task	For more information
Installing the Oracle Identity Management 11g Release 1 (11.1.1.3.0) suite containing Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Authorization Policy Manager, and Oracle Identity Navigator on the Windows machine where you want to install only Design Console	See Installing OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0).
Configuring Oracle Identity Manager Server on a local or remote machine **Note**: The Oracle Identity Manager Server must be up and running when you configure only Design Console.	See Configuring OIM Server.
Configuring Oracle Identity Manager Design Console on the Windows machine where you want to install only Design Console	See Configuring OIM Design Console.
Completing any post-configuration steps	See Post-Configuration Steps.

> **Note:** For more information, see Prerequisites for Configuring Only OIM Design Console on a Different Machine.

6.6 Configuring OIM Design Console

This topic describes how to install and configure only Oracle Identity Manager (OIM) 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

6.6.1 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.

6.6.2 Components Deployed

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

6.6.3 Dependencies

The installation and configuration in this section depends on the installation of Oracle Identity Management 11*g* software and on the Oracle Identity Manager Server. For more information, see Installing OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0) and Configuring OIM Server.

6.6.4 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 Prerequisites for Configuring Only OIM Design Console on a Different Machine, are satisfied.

2. On the machine where Design Console should be configured, start the Oracle Identity Manager Configuration Wizard, as described in 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 the topic "Performing Silent Installations" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

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 Locating 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 Starting the Oracle Identity Manager 11g Configuration Wizard.

6.6.5 Post-Configuration Steps

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

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_11
   ```

   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_11, 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. At the DOS command prompt, type the following command:

```
java -jar <MW_HOME>modules/com.bea.core.jarbuilder_
1.5.0.0.jar
```

This command generates the `wlfullclient.jar` file.

3. Copy the `wlfullclient.jar` file to the `<Oracle_
   IDM2>\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 `<IDM_Home>\designconsole\` directory.

6. Log in to the Design Console with your Oracle Identity Manager user name and
   password.

6.7 Configuring OIM Remote Manager

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

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure

6.7.1 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.

6.7.2 Components Deployed

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

6.7.3 Dependencies

The installation and configuration in this section depends on the installation of Oracle
Identity Management 11*g* software. For more information, see Installing OIM, OAM,
OAAM, OAPM, and OIN (11.1.1.3.0) and Prerequisites for Configuring Only OIM
Remote Manager on a Different Machine.

6.7.4 Procedure

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

1. Ensure that all the prerequisites, described in Prerequisites for Configuring Only
   OIM Remote Manager on a Different Machine, are satisfied.

2. On the machine where Remote Manager should be configured, start the Oracle
   Identity Manager Configuration Wizard, as described in 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 the topic "Performing Silent Installations" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

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 Locating 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 Starting the Oracle Identity Manager 11g Configuration Wizard.

7

Verifying the Installed Components

This chapter describes how to verify the installation of Oracle Identity Management 11*g* Release 1 (11.1.1) components.

It contains the following sections:

- Verifying OID, OVD, ODSM, ODIP, and OIF (11.1.1.4.0)
- Verifying OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0)

7.1 Verifying OID, OVD, ODSM, ODIP, and OIF (11.1.1.4.0)

This topic describes how to verify Oracle Internet Directory (OID), Oracle Virtual Directory (OVD), Oracle Directory Services Manager (ODSM), Oracle Directory Integration Platform (ODIP), and Oracle Identity Federation (OIF) that you installed.

It includes the following sections:

- Oracle Internet Directory or Oracle Virtual Directory
- Oracle Directory Integration Platform
- Oracle Directory Services Manager
- Oracle Identity Federation

7.1.1 Oracle Internet Directory or Oracle Virtual Directory

Verify an Oracle Internet Directory or an Oracle Virtual Directory installation by:

- Executing the $*ORACLE_INSTANCE*/bin/opmnctl status -l command. For example, if Oracle Internet Directory is configured then the following result can be seen:

```
Processes in Instance: asinst_1
-------------------------------+-------------------+--------+----------+---
---------+----------+-----------+------
ias-component                  | process-type      |    pid | status   |
uid | memused |   uptime | ports
-------------------------------+-------------------+--------+----------+---
---------+----------+-----------+------
oid1                           | oidldapd          |  24032 | Alive    |
582907955 |  113004 |   0:00:41 | N/A
oid1                           | oidldapd          |  24024 | Alive    |
582907954 |   56288 |   0:00:42 | N/A
oid1                           | oidmon            |  24001 | Alive    |
582907953 |   50232 |   0:00:43 | LDAPS:3131,LDAP:3060
EMAGENT                        | EMAGENT           |  24000 | Alive    |
582907952 |    5852 |   0:00:43 | N/A
```

- Executing the `$ORACLE_HOME/bin/ldapbind` command on the non-SSL and SSL ports. For example:

  On Non-SSL ports:

  ```
  $ORACLE_HOME/bin/ldapbind -h <hostname> -p <port> -D
  cn=orcladmin -w <password>
  ```

  On SSL ports:

  ```
  $ORACLE_HOME/bin/ldapbind -h <hostname> -p <port> -D
  cn=orcladmin -w <password> -U 1
  ```

7.1.2 Oracle Directory Integration Platform

Verify the Oracle Directory Integration Platform installation using the `dipStatus` command located in the $*ORACLE_HOME*/bin/ directory.

> **Note:** You must set the *WL_HOME* and *ORACLE_HOME* environment variables before executing the `dipStatus` command.

The following is the syntax for the `dipStatus` command:

```
$ORACLE_HOME/bin/dipStatus -h HOST -p PORT -D wlsuser [-help]
```

- `-h | -host` identifies the Oracle WebLogic Server where Oracle Directory Integration Platform is deployed.

- `-p | -port` identifies the listening port of the Oracle WebLogic Managed Server where Oracle Directory Integration Platform is deployed.

- `-D | -wlsuser` identifies the Oracle WebLogic Server login ID.

> **Note:** You will be prompted for the Oracle WebLogic Server login password. You cannot provide the password as a command-line argument.
>
> Best security practice is to provide a password only in response to a prompt from the command. If you must execute `dipStatus` from a script, you can redirect input from a file containing the Oracle WebLogic Server password. Use file permissions to protect the file and delete it when it is no longer necessary.

7.1.3 Oracle Directory Services Manager

To verify the Oracle Directory Services Manager installation, enter the following URL into your browser's address field:

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

- *host* represents the name of the WebLogic Managed Server hosting Oracle Directory Services Manager.

- *port* represents the WebLogic Managed Server listen port. You can determine the exact port number by examining the

  ```
  $MW_HOME/ORACLE_IDENTITY_MANAGEMENT_DOMAIN/servers/MANAGED_
  SERVER/data/nodemanager/MANAGED_SERVER.url
  ```

Oracle Directory Services Manager is installed and running if the Welcome to Oracle Directory Services Manage screen appears.

> **Note:** While the appearance of the Welcome screen verifies Oracle Directory Services Manager is installed and running, you cannot connect to an Oracle Internet Directory or Oracle Virtual Directory from Oracle Directory Services Manager without the appropriate directory server credentials.

7.1.4 Oracle Identity Federation

Verify the Oracle Identity Federation installation by:

- Accessing the Oracle Identity Federation metadata at the following URL. Oracle Identity Federation was installed and the Oracle Identity Federation server is running if you can access the metadata.

  ```
  http://host:port/fed/sp/metadata
  ```

> **Note:** *host* represents the name of the WebLogic Managed Server where Oracle Identity Federation was installed. *port* represents the listen port on that WebLogic Managed Server.

- Accessing Fusion Middleware Control to verify that Oracle Identity Federation is available and running. For more information, see "Getting Started Using Oracle Enterprise Manager Fusion Middleware Control" in the Oracle Fusion Middleware Administrator's Guide.

7.2 Verifying OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0)

This topic describes how to verify Oracle Identity Manager (OIM), Oracle Access Manager (OAM), Oracle Adaptive Access Manager (OAAM), Oracle Authorization Policy Manager (OAPM), and Oracle Identity Navigator (OIN) that you installed.

It includes the following sections:

- Verifying the OIM Installation
- Verifying the OAM Installation
- Verifying the OAAM Installation
- Verifying the OAPM Installation
- Verifying the OIN Installation

7.2.1 Verifying the OIM Installation

Before you can verify the Oracle Identity Manager (OIM) 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`.

7.2.2 Verifying the OAM Installation

After completing the installation process, including post-installation steps, you can
verify the installation and configuration of Oracle Access Manager (OAM) 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.

7.2.3 Verifying the OAAM Installation

After completing the installation process, including post-installation steps, you can verify the installation and configuration of Oracle Adaptive Access Manager (OAAM) 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 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 URL: `http://<host>:<port>/oaam_admin`

4. Log in to the Oracle Adaptive Access Manager Server using the URL: `https://<host>:<sslport>:oaam_server`

7.2.4 Verifying the OAPM Installation

After completing the installation and configuration of Oracle Authorization Policy Manager (OAPM), including the post-installation steps, you can verify the installation as follows:

1. Verify whether a login page appears when you access `http://<hostname>:<apm-port>/apm`.

2. After you log in, the Authorization Policy Manager Console is displayed. The home page should display three tabs: **Authorization Management**, **System Configuration**, and **Policy Upgrade Management**.

3. On the home page, ensure that the **Authorization Management** tab is active. Click **Search - External Roles** in the **Global** section on the home page. The Search - External Roles page is displayed.

These results indicate that your installation of Oracle Authorization Policy Manager was successful.

7.2.5 Verifying the OIN Installation

To verify the installation of Oracle Identity Navigator (OIN), 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 **Edit** 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.

Deinstalling and Reinstalling Oracle Identity Management

This appendix provides information about deinstalling and reinstalling Oracle Identity Management 11*g* Release 1 (11.1.1.3.0). It contains the following topics:

- Deinstalling Oracle Identity Management
- Reinstalling Oracle Identity 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.

A.1 Deinstalling Oracle Identity Management

This topic contains procedures for deinstalling Oracle Identity Management and contains the following sections:

- Deinstalling the Oracle Identity Management Oracle Home
- Deinstalling the Oracle Common Home
- Deinstalling Applications Registered with Oracle Single Sign-On 10g Release 10.1.4.3.0

A.1.1 Deinstalling the Oracle Identity 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 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 Management will not remove any WebLogic domains that you have created—it only removes the software in the Oracle Identity 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 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 Management Oracle Home using the graphical, screen-based deinstaller:

1. Verify your Oracle Identity Management Oracle Home is not in use by an existing domain.

2. Stop all processes that use the Oracle Identity Management Oracle Home.

3. Open a command prompt and move (cd) into the *IDENTITY_MANAGEMENT_ ORACLE_HOME*/oui/bin directory (UNIX) or the *IDENTITY_MANAGEMENT_ ORACLE_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**.

   - If you are deinstalling Oracle Internet Directory, Oracle Virtual Directory, Oracle Directory Services Manager, Oracle Directory Integration Platform, or Oracle Identity Federation, the Select Deinstallation Type screen appears.

     Select the deinstallation type you want to perform. Table A–1 lists and describes each of the deinstallation types:

Table A–1   Deinstallation Types

Type	Description
Deinstall Oracle Home	Select this option to deinstall the binaries contained in the listed Oracle Identity Management Oracle Home.
	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.
	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.
	If you select this option, the Specify Instance Location screen appears next where you identify the instances you want to deinstall.

   Regardless of the option you choose and the subsequent screens that appear, you will arrive at the Deinstall Progress screen, which shows the progress and status of the deinstallation. If you want to quit before the deinstallation is completed, click **Cancel**.

Click **Finish** after the deinstallation progresses to 100%. The Deinstallation Complete screen appears.

- If you are deinstalling Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Authorization Policy Manager, and Oracle Identity Navigator, the Deinstall Oracle Home screen appears.

  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. If you want to quit before the deinstallation is completed, click **Cancel**.

  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.

A.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.

2. Deinstall your Oracle Identity Management Oracle Home by performing the steps in Deinstalling Oracle Identity Management.

3. Open a command prompt and move (cd) into the *ORACLE_COMMON*/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.

A.1.3 Deinstalling Applications Registered with Oracle Single Sign-On 10*g* Release 10.1.4.3.0

To deinstall a partner application registered with Oracle Single Sign-On 10*g* Release 10.1.4.3.0, you must manually deregister the partner application from Oracle Single Sign-On. Refer to the "Reregister mod_osso on the single sign-on middle tiers" section in Chapter 9 of the *Oracle Application Server Single Sign-On Administrator's Guide 10g Release 10.1.4.0.1* available at:

http://www.oracle.com/technetwork/indexes/documentation/index.html

A.2 Reinstalling Oracle Identity Management

Perform the following steps to reinstall Oracle Identity Management:

1. Verify the directory you want to reinstall Oracle Identity Management into does not contain an existing Oracle Identity Management instance. If it does, you must deinstall it before reinstalling. You cannot reinstall Oracle Identity Management 11*g* Release 1 (11.1.1) in a directory that contains an existing Oracle Identity Management instance.

2. Reinstall Oracle Identity Management as if it was the first installation by performing the steps in the appropriate procedure in this guide.

B Starting and Stopping the Oracle Stack

You must start and 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

> **Note:** When executing the startManagedWebLogic and stopManagedWebLogic scripts described in the following topics:
>
> - The default value for *DOMAIN_NAME* is IDMDomain
> - *SERVER_NAME* represents the name of the WebLogic Managed Server. The default value for the Oracle Directory Integration Platform and Oracle Directory Services Manager WebLogic Managed Server is wls_ods1. The default value for the Oracle Identity Federation WebLogic Managed Server is wls_oif1.
> - 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.

B.1 Starting the Stack

Start the stack components in the following order:

1. Start the WebLogic Administration Server by executing the following command:

   `MW_HOME/user_projects/domains/DOMAIN_NAME/bin/startWebLogic.sh`

2. 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`

3. Start WebLogic managed components, such as Oracle Directory Integration Platform, Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Identity Federation, and Oracle Directory Services Manager, by executing the following command:

   `MW_HOME/user_projects/domains/DOMAIN_NAME/bin/startManagedWebLogic.sh\`
   `SERVER_NAME {ADMIN_URL}`

   > **Note:** You can view the status of WebLogic managed components with Fusion Middleware Control.

B.2 Stopping the Stack

Stop the stack components in the following order:

1. Stop WebLogic managed components, such as Oracle Identity Manager, Oracle Access 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 the WebLogic Administration Server by executing the following command:

   ```
   MW_HOME/user_projects/domains/DOMAIN_NAME/bin/stopWebLogic.sh
   ```

3. Stop system components, such as Oracle Internet Directory and Oracle Virtual Directory, by executing the following command:

   ```
   ORACLE_INSTANCE/bin/opmnctl stopall
   ```