Oracle® Fusion Middleware

Installation Guide for Oracle Identity Management

11*g* Release 1 (11.1.1)

E12002-06

April 2011

ORACLE®

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

E12002-06

Primary Author: Nisha Singh

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

Contents

3 Preparing to Install Oracle Identity Management

4 Performing Common Installation Tasks

Part II Installing and Configuring OID, OVD, ODSM, ODIP, and OIF (11.1.1.5.0)

5 Installing OID, OVD, ODSM, ODIP, and OIF (11.1.1.5.0)

6 Configuring Oracle Internet Directory

7 Configuring Oracle Virtual Directory

15 Configuring Oracle Identity Navigator

16 Configuring Oracle Identity Manager

17 Configuring Oracle Access Manager

H Oracle Identity Manager Configuration Screens

I Software Deinstallation Screens

Preface

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

Audience

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

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

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

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

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

---

Note: Printed documentation is available for sale from the Oracle Store Web site at the following URL:

http://oraclestore.oracle.com/

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

Oracle Fusion Middleware

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

Oracle Identity Management

- *Oracle Fusion Middleware Getting Started with Oracle Identity Management*
- *Oracle Fusion Middleware User Reference for Oracle Identity Management*

Installing and Upgrading

- *Oracle Fusion Middleware Installation Planning Guide*
- *Oracle Fusion Middleware Quick Installation Guide for Oracle Identity Management*
- *Oracle Fusion Middleware Upgrade Planning Guide*
- *Oracle Fusion Middleware Upgrade Guide for Oracle Identity Management*
- *Oracle Fusion Middleware Getting Started With Installation for Oracle WebLogic Server*
- *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*

High Availability

- *Oracle Fusion Middleware High Availability Guide*
- *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management*

Oracle Internet Directory

- *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*
- *Oracle Fusion Middleware Application Developer's Guide for Oracle Identity Management*

Oracle Directory Integration Platform

- *Oracle Fusion Middleware Integration Guide for Oracle Identity Management*

Oracle Virtual Directory

- *Oracle Fusion Middleware Administrator's Guide for Oracle Virtual Directory.*

Oracle Directory Services Manager

- *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Virtual Directory*

Oracle Identity Federation

- *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation.*

Oracle Single Sign-On

- *Oracle Application Server Single Sign-On Administrator's Guide 10g Release 10.1.4.0.1* available at:

  `http://www.oracle.com/technology/documentation/oim1014.html`

Oracle Delegated Administration Services

- *Oracle Identity Management Guide to Delegated Administration 10g Release 10.1.4.0.1* available at:

  `http://www.oracle.com/technology/documentation/oim1014.html`

Oracle Fusion Middleware Repository Creation Utility

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

Oracle Identity Manager

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

Oracle Access Manager

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

Oracle Adaptive Access Manager

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

Oracle Authorization Policy Manager

- *Oracle Fusion Middleware Authorization Policy Manager Administrator's Guide*

Oracle Identity Navigator

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

Conventions

The following text conventions are used in this document:

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

Part I

Introduction and Preparation

Part I introduces Oracle Identity Management 11g Release 1 (11.1.1) installation and describes how to perform preparatory and common installation tasks. It contains the following chapters:

1

Understanding Oracle Identity Management

This chapter provides a brief overview of Oracle Identity Management 11*g* Release 1 (11.1.1.3.0) and this guide. This chapter includes the following topics:

- What is Oracle Fusion Middleware?
- What is Oracle Identity Management?
- Oracle Identity Management 11g Release 1 (11.1.1.5.0) Components
- Oracle Identity Management 11g Release 1 (11.1.1.3.0) Components
- What Does This Guide Cover?

> **See:** The "Related Documents" section in this guide's Preface for a list of documents that provide additional information about the topics described in this chapter.

1.1 What is Oracle Fusion Middleware?

Oracle Identity Management is part of Oracle Fusion Middleware. Oracle Fusion Middleware is a collection of standards-based software products that spans a range of tools and services: From Java EE and developer tools, to integration services, business intelligence, and collaboration. Oracle Fusion Middleware offers complete support for development, deployment, and management.

1.1.1 What is Oracle Enterprise Manager Fusion Middleware Control?

Oracle Enterprise Manager Fusion Middleware Control is a Web browser-based graphical user interface that you can use to monitor and administer Oracle Fusion Middleware components, including Oracle Identity Management components, that are installed in Oracle WebLogic Server domains.

> **Note:** When you install Oracle Identity Management components in a new domain, the Fusion Middleware Control management component is included.

1.2 What is Oracle Identity Management?

Oracle Identity Management enables enterprises to manage the end-to-end lifecycle of user identities across all enterprise resources—both within and beyond the firewall. With Oracle Identity Management, you can deploy applications faster, apply the most

granular protection to enterprise resources, automatically eliminate latent access privileges, and much more.

Oracle Corporation leads the industry with award-winning Identity Management offerings that constitute the most comprehensive solution offered by any vendor, including:

- Web Access Control
- Adaptive Access Control
- Identity Federation
- Identity Administration
- User Access Provisioning
- Role Management
- Authorization Policy Management
- Directory Services

For more information about Oracle Identity Management, refer to the Identity Management home page on Oracle Corporation's Web site at:

http://www.oracle.com/identity

1.3 Oracle Identity Management 11*g* Release 1 (11.1.1.5.0) Components

Oracle Identity Management 11*g* Release 1 (11.1.1.5.0) includes the following components:

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

Note: For more information on Installing and Configuring OID, OVD, ODSM, ODIP, and OIF (11.1.1.5.0), see Part II.

1.3.1 Oracle Single Sign-On and Oracle Delegated Administration Services Certification for 11*g* Release 1 (11.1.1.5.0)

Oracle Single Sign-On and Oracle Delegated Administration Services Release 10*g* are required components for Oracle Portal, Forms, Reports and Discoverer Release 10*g* and Release 11*g*.

There are no 11*g* Release 1 (11.1.1) versions of Oracle Single Sign-On and Oracle Delegated Administration Services. However, both Oracle Single Sign-On and Oracle Delegated Administration Services Release 10*g* (10.1.4.3.0) are certified for use with Oracle Internet Directory 11*g* Release 1 (11.1.1).

If you are running Oracle Single Sign-On or Oracle Delegated Administration Services Release 10*g*, you can either:

- Continue using Oracle Single Sign-On and Oracle Delegated Administration Services Release 10g with Oracle Internet Directory Release 10g.

or

- Upgrade to Oracle Internet Directory 11g Release 1 (11.1.1) to use its new features.

  See: The following for more information:

  - Chapter 11, "Installing Oracle Single Sign-On and Oracle Delegated Administration Services Against Oracle Internet Directory."
  - Chapter 10, "Configuring Single Sign-On in Oracle Fusion Middleware," in the *Oracle Fusion Middleware Security Guide*, for recommended single sign-on solutions for Oracle Fusion Middleware.

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

Oracle Identity Management 11*g* Release 1 (11.1.1.3.0) includes the following components:

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

Note: For more information on Installing and Configuring OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0), see Part III.

1.5 What Does This Guide Cover?

This topic describes the scope of information in this guide and how to use it. This topic includes the following sections:

- Using This Guide
- Upgrading to OID, OVD, ODSM, ODIP, and OIF (11.1.1.5.0)
- Upgrading to OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0)
- Installing OID, OVD, ODSM, ODIP, and OIF (11.1.1.5.0) for High Availability
- Installing OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0) for High Availability

1.5.1 Using This Guide

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

1. Install single instances of Oracle Identity Management 11*g* Release 1 (11.1.1.3.0) components.
2. Verify the installation was successful.
3. Get started with the component after installation.

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

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

Part II of this guide explains how to install Oracle Internet Directory, Oracle Virtual Directory, Oracle Directory Services Manager, Oracle Directory Integration Platform, and Oracle Identity Federation Management by using the Oracle Identity Management 11.1.1.5.0 Installer and the Oracle Identity Management Configuration Wizard.

Part III of this guide explains how to install Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Authorization Policy Manager, and Oracle Identity Navigator by using the Oracle Identity and Access Management 11.1.1.3.0 Installer and the Oracle Fusion Middleware Configuration Wizard. The Oracle Identity Management 11*g* Configuration Wizard is used for configuring Oracle Identity Manager only.

The following is a list of recommendations on how to use the information in this guide to install Oracle Identity Management 11*g* Release 1 (11.1.1.3.0):

1. Review Chapter 2, "Understanding the Oracle Identity Management Installation," for context.
2. Review Chapter 3, "Preparing to Install Oracle Identity Management," for information about what you should consider before you deploy Oracle Identity Management.
3. Review Chapter 4, "Performing Common Installation Tasks," to understand the tasks that you must perform for most deployments. Understanding this information before you start will expedite and simplify the deployment process.
4. Install, verify, and get started with your Oracle Identity Management component by referring to its specific chapter in this guide.
5. Use the appendixes in this guide as needed.

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

1.5.2 Upgrading to OID, OVD, ODSM, ODIP, and OIF (11.1.1.5.0)

This guide does not explain how to upgrade legacy versions of Oracle Identity Management components, including any previous database schemas, to OID, OVD, ODSM, ODIP, and OIF (11.1.1.5.0). To upgrade a legacy version of an Oracle Identity Management component, refer to the following documents:

- *Oracle Fusion Middleware Upgrade Planning Guide*
- *Oracle Fusion Middleware Upgrade Guide for Oracle Identity Management*

1.5.3 Upgrading to OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0)

This guide does not explain how to upgrade legacy versions of Oracle Identity Management components, including any previous database schemas, to OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0). To upgrade a legacy version of an Oracle Identity Management component, refer to the following documents:

- *Oracle Fusion Middleware Upgrade Planning Guide*
- *Oracle Fusion Middleware Upgrade Guide for Oracle Identity Management*

1.5.4 Installing OID, OVD, ODSM, ODIP, and OIF (11.1.1.5.0) for High Availability

This guide does not explain how to install OID, OVD, ODSM, ODIP, and OIF (11.1.1.5.0) components in High Availability (HA) configurations. To install an Oracle Identity Management component in a High Availability configuration, refer to the following documents:

- *Oracle Fusion Middleware High Availability Guide*
- *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management*

1.5.5 Installing OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0) for High Availability

This guide does not explain how to install OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0) components in High Availability (HA) configurations. To install an Oracle Identity Management component in a High Availability configuration, refer to the following documents:

- *Oracle Fusion Middleware High Availability Guide*
- *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management*

2

Understanding the Oracle Identity Management Installation

This chapter provides an overview of the Oracle Identity Management 11*g* Release 1 (11.1.1) installation. This chapter includes the following topics:

- Overview and Structure of Oracle Identity Management 11g Installation
- Overview of OID, OVD, ODSM, ODIP, and OIF (11.1.1.5.0) Installation
- Overview of OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0) Installation

> **Note:** For information about installing the 11*g* (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 11.1.1.5.0, see Overview of OID, OVD, ODSM, ODIP, and OIF (11.1.1.5.0) Installation.
>
> For information about 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 Overview of OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0) Installation.

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

This section discusses the following topics:

- Overview
- Structure of the Installation

2.1.1 Overview

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

- Oracle Identity Management 11g Release 1 (11.1.1.5.0)
- Oracle Identity and Access Management 11g Release 1 (11.1.1.3.0)

Oracle Identity Management 11*g* Release 1 (11.1.1.5.0)

To install Oracle Identity Management 11*g* Release 1 (11.1.1.5.0), you must install Oracle Identity Management 11g Release 1 (11.1.1.2.0) first.

To install Oracle Identity Management 11g 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 Directory (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 11.1.1.5.0 using the `ofm_idm_win_11.1.1.5.0_32_disk1_1of1.zip` (for **Windows**) or `ofm_idm_linux_11.1.1.5.0_32_disk1_1of1.zip` (for **Linux**)

> **Note:** See Part II, "Installing and Configuring OID, OVD, ODSM, ODIP, and OIF (11.1.1.5.0)" in this guide for installing and configuring these products.

Oracle Identity and Access Management 11*g* Release 1 (11.1.1.3.0)

To install Oracle Identity and Access Management 11g Release 1 (11.1.1.3.0), 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 Identity Manager (OIM)
- Oracle Access Manager (OAM)
- Oracle Authorization Policy Manager (OAPM)
- Oracle Identity Navigator (OIN)
- Oracle Adaptive Access Manager (OAAM)

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

2.1.2 Structure of the Installation

You can install both of the Oracle Identity Management 11.1.1.3.0 and 11.1.1.5.0 products under a common Middleware Home directory. When you install these suites on the same machine, two Oracle Home (also referred to as IDM_Home in this guide) directories are created on the machine. For information about identifying installation directories, see Section 4.1.3, "Identifying Installation Directories" and Section 4.2.4, "Identifying Installation Directories".

Note that two IDM_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.

2.2 Overview of OID, OVD, ODSM, ODIP, and OIF (11.1.1.5.0) Installation

This section discusses the following topics:

- Installation Roadmap
- Installation Types: "Install Software - Do Not Configure" vs. "Install and Configure"
- Understanding Oracle WebLogic Server Administration Domain Options
- Installing Components on Separate Systems
- Executing the oracleRoot.sh Script on UNIX Platforms
- Understanding the State of Oracle Identity Management Components After Installation

2.2.1 Installation Roadmap

Table 2–1 describes the high-level tasks for installing and configuring Oracle Identity Management. The table also provides information on where to get more details about each task.

Table 2–1 Tasks in the Oracle Identity Management Installation Procedure

Task	Description	Documentation	Mandatory or Optional?
Task 1 - Prepare your environment for installation.	Ensure that your system environment meets the general installation requirements for Oracle Fusion Middleware as well as Oracle Identity Management and RCU.	For system requirements information, go to: `http://www.oracle.com/technetwork/middleware/ias/downloads/fusion-requirements-100147.html` For certification information, go to:	Mandatory
Task 2 - Run RCU to create the necessary schemas.	Oracle Identity Management components require schemas that must be installed in an Oracle database. You create and load these schemas in your database by using RCU.	Make sure you have a supported Oracle database up and running. See `http://www.oracle.com/technetwork/middleware/ias/downloads/fusion-certification-100350.html` for more information. Instructions for creating the schema are provided in "Running Oracle Fusion Middleware Repository Creation Utility (RCU)" in the *Oracle Fusion Middleware Repository Creation Utility User's Guide*. In addition, refer to Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU) in this guide.	Mandatory
Task 3 - Install Oracle WebLogic Server and create a Middleware home.	Oracle Identity Management requires a Middleware home directory. The Middleware home is created during the Oracle WebLogic Server 10.3.5 installation. The WebLogic Server installer also creates the WebLogic home directory within the Oracle Middleware home directory.	Installation instructions are provided in *Oracle WebLogic Server Installation Guide*. For more information about the Middleware home and WebLogic home directories, see *Oracle Fusion Middleware Concepts Guide*.	Mandatory

Table 2–1 (Cont.) Tasks in the Oracle Identity Management Installation Procedure

Task	Description	Documentation	Mandatory or Optional?
Task 4 - Install but do not configure Oracle Identity Management	Use the installer to install Oracle Identity Management 11.1.1.2.0 Choose the **Install Software - Do Not Configure** option on the Select Installation Type Screen.	See Installing OID, OVD, ODSM, ODIP, and OIF (11.1.1.5.0). For more information about the installation types, see Installation Types: "Install Software - Do Not Configure" vs. "Install and Configure".	Mandatory
Task 5 - Update your software.	Run the Patch Set Installer to update your software to Oracle Identity Management 11.1.1.5.0.	See "Applying the Latest Oracle Fusion Middleware Patch Set with the Patch Set Installers" in *Oracle Fusion Middleware Patching Guide*.	Mandatory
Task 6 - Configure Oracle Identity Management	After patching, run the Configuration Tool to configure your Oracle Identity Management components.	See the following topics in this guide: ■ Only OID in an Existing WebLogic Domain ■ Only OID Without a WebLogic Domain ■ OID with ODSM and Fusion Middleware Control in a New WebLogic Domain ■ OID with ODIP, ODSM, and Fusion Middleware Control in a New WebLogic Domain ■ OVD with ODSM and Fusion Middleware Control in a New WebLogic Domain ■ Only OVD in an Existing WebLogic Domain ■ Only OVD Without a WebLogic Domain ■ Performing Basic OIF Configurations ■ Performing Advanced OIF Configurations ■ ODIP with Fusion Middleware Control in a New WebLogic Domain ■ Only ODIP in an Existing WebLogic Domain ■ Configuring ODIP when OID is Running in SSL Mode 2 - Server Only Authentication	Mandatory

2.2.2 Installation Types: "Install Software - Do Not Configure" vs. "Install and Configure"

The Select Installation Type screen in the Installer presents two options: **Install and Configure** and **Install Software - Do Not Configure**. This section describes both options:

- Understanding the "Install Software - Do Not Configure" Option
- Understanding the "Install and Configure" Option

2.2.2.1 Understanding the "Install Software - Do Not Configure" Option

Choose the **Install Software - Do Not Configure** option to install Oracle Identity Management components without configuring them during installation. If you choose the **Install Software - Do Not Configure** option, the Installer installs the component software and then closes. Oracle Identity Management components will *not* start running after deploying them using the **Install Software - Do Not Configure** option, as additional configuration is needed.

After you install components using the **Install Software - Do Not Configure** option, you can configure them at a later time using the Oracle Identity Management Configuration Wizard. To start the Oracle Identity Management Configuration Wizard, execute the *ORACLE_HOME*`/bin/config.sh` script (config.bat on Windows).

Important: To install the latest Oracle Identity Management software, you must choose the **Install Software - Do Not Configure** installation type option, for Oracle Identity Management 11.1.1.2.0.

2.2.2.2 Understanding the "Install and Configure" Option

The **Install and Configure** option allows you to install Oracle Identity Management components and simultaneously configure some of their fundamental elements, such as passwords, user names, and so on. Oracle Identity Management components start running and are immediately ready for use after deploying them using the **Install and Configure** option.

Note: Do not choose the **Install and Configure** option for Oracle Identity Management 11.1.1.2.0, if you want to install the latest Oracle Identity Management software.

2.2.3 Understanding Oracle WebLogic Server Administration Domain Options

During installation, you have several options for choosing how the Oracle Identity Management components are installed in relation to an Oracle WebLogic Server administration domain. A domain includes a special WebLogic Server instance called the Administration Server, which is the central point from which you configure and manage all resources in the domain.

This section describes each domain option for installing Oracle Identity Management components:

- Create New Domain
- Extend Existing Domain
- Expand Cluster
- Configure Without a Domain

See: The "Understanding Oracle WebLogic Server Domains" chapter in the *Oracle Fusion Middleware Understanding Domain Configuration for Oracle WebLogic Server* guide for more information about Oracle WebLogic Server administration domains.

2.2.3.1 Create New Domain

Select the **Create New Domain** option to create a new Oracle WebLogic Server administration domain and install Oracle Identity Management components in it.

When you install Oracle Identity Management components in a new domain, the Fusion Middleware Control management component and the Oracle WebLogic Administration Server are automatically deployed with them.

2.2.3.2 Extend Existing Domain

Select the **Extend Existing Domain** option to install Oracle Identity Management components in an existing Oracle WebLogic Server administration domain. When you install Oracle Identity Management components using this option, they are essentially "joining" an existing domain.

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

If you want to install and configure Oracle Identity Management components in an existing Oracle WebLogic Server administration domain, by using either the Installer or the Oracle Identity Management Configuration Wizard, the existing domain must have been created using the Oracle Identity Management 11*g* Release 1 (11.1.1.5.0) Installer. You cannot extend an existing domain for Oracle Identity Management components if the domain was created by another program, such as the Oracle SOA Installer or the Oracle Fusion Middleware Configuration Wizard.

> **Note:** When you install components using the **Extend Existing Domain** option, you must provide some credentials for the existing domain, including the user name for the domain. You must enter the user name in ASCII characters only.

2.2.3.3 Expand Cluster

Select the **Expand Cluster** option to install Oracle Identity Management components in an Oracle WebLogic Server cluster for High Availability (HA). This document does not explain how to install Oracle Identity Management components in HA configurations. Refer to the following documents for more information:

- *Oracle Fusion Middleware High Availability Guide*
- *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management*

2.2.3.4 Configure Without a Domain

Select the **Configure without a Domain** option to install Oracle Identity Management components and configure them to be without domain membership.

> **Note:** Only the Oracle Internet Directory and Oracle Virtual Directory components are certified for installation without a domain.

For Oracle Internet Directory, the **Configure without a Domain** option is appropriate for environments that have *both* of the following conditions:

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

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

For Oracle Virtual Directory, the **Configure without a Domain** option is appropriate if you want to register Oracle Virtual Directory with a remote WebLogic Administration Server for management purposes, but you do not want to install Oracle WebLogic Server locally.

2.2.4 Installing Components on Separate Systems

You can install Oracle Fusion Middleware instances on separate systems. You can also distribute Oracle Fusion Middleware components over multiple systems, which is especially useful for Oracle Identity Management components. You might want distribute components to improve performance, security, scalability, and availability of Oracle Identity Management services.

The following are two (of many) examples of Oracle Identity Management deployments that benefit from distributing components over multiple systems:

- Oracle Internet Directory on one system, and Oracle Directory Services Manager and Oracle Directory Integration Platform on a separate system.
- Oracle Identity Management components use an Oracle Database to contain the Oracle Metadata Repository. The Oracle Identity Management components and the Oracle Database are installed on separate systems.

Note: If you install Oracle Identity Management components on a separate system from the database containing the Oracle Metadata Repository, the Oracle Identity Management components will need network access to the repository.

See: The following documents if you want to configure more than one Oracle Internet Directory against the same Oracle Metadata Repository:

- *Oracle Fusion Middleware Installation Planning Guide*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*

2.2.5 Executing the oracleRoot.sh Script on UNIX Platforms

During installation on UNIX platforms, the Installer prompts you to log in as the root user and run the `oracleRoot.sh` script. You must log in as the root user because the script creates files, edits files, and changes the permissions of certain Oracle executable files in the `<Oracle_IDM_Home>/bin` directory.

If the `oracleRoot.sh` script finds files of the same name, it prompts you to indicate whether or not to override the existing files. Back up the existing files (you can do this from another window), then overwrite them.

2.2.6 Understanding the State of Oracle Identity Management Components After Installation

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

- Default SSL Configurations

- Default Passwords
- Ports Assigned Using Auto Port Configuration

2.2.6.1 Default SSL Configurations

By default, Oracle Internet Directory and Oracle Virtual Directory are installed with SSL configured. You must configure SSL for the Oracle WebLogic Administration Server and Oracle WebLogic Managed Server after installation.

> **See:** The *Oracle Fusion Middleware Administrator's Guide* for more information.

2.2.6.2 Default Passwords

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

> **See:** The following documents for information about changing passwords for Oracle Identity Management components:
>
> - *Oracle Fusion Middleware Administrator's Guide*
> - Component-specific guides listed in the "Related Documents" section in this guide's Preface.

2.2.6.3 Ports Assigned Using Auto Port Configuration

When you use the Auto Port Configuration option during installation, the Installer follows specific steps to assign ports. The following information describes the default ports and port assignment logic the Installer uses to assign ports for various Oracle Identity Management components when you use the Auto Port Configuration option during installation.

- **Oracle Virtual Directory:**
  - Non-SSL port: 6501
  - SSL port: 7501
  - Admin port: 8899
  - HTTP port: 8080

  First, the Installer attempts to assign the default port. If the default port is unavailable, the Installer tries ports within a range of 50 from the default port. For example, when the Installer assigns the non-SSL port for Oracle Virtual Directory, it first attempts to assign 6501. If 6501 is unavailable, it tries ports from 6501 to 6551. The Installer uses this approach to assign all Oracle Virtual Directory ports.
- **Oracle Internet Directory:**
  - Non-SSL port: 3060
  - SSL port: 3131

  First, the Installer attempts to assign default ports. If the non-SSL port is unavailable, the Installer tries ports from 3061 to 3070, then from 13060 to 13070. Similarly, the Installer first attempts to assign 3131 as the SSL port, then ports from 3132 to 3141, and then from 13131 to 13141.
- **Oracle Identity Federation**: 7499

First, the Installer attempts to assign the default port. If the default port is unavailable, the Installer tries ports in increments of one, that is: 7500, then 7501, then 7502, and so on. The Installer tries ports up until 9000 to find an available port.

- **Oracle Directory Services Manager**: 7005

  First, the Installer attempts to assign the default port. If the default port is unavailable, the Installer tries ports in increments of one, that is: 7006, then 7007, then 7008, and so on. The Installer tries ports up until 9000 to find an available port.

- **Oracle WebLogic Administration Server**: 7001

2.3 Overview of OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0) Installation

This section discusses the following topics:

2.3.1 Installation Roadmap

Table 2–2 lists the tasks required to install and configure Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Authorization Policy Manager, and Oracle Identity Navigator.

Table 2–2 Installation Flow for Oracle Identity Management

No.	Task	Description
1	Review installation concepts in the Installation Planning Guide.	Read the *Oracle Fusion Middleware Installation Planning Guide*, which describes the process for various users to install or upgrade to Oracle Fusion Middleware 11g (11.1.1.3) depending on the user's existing environment.

2	Review the system requirements and certification documents to ensure that your environment meets the minimum installation requirements for the components you are installing.	Read the *System Requirements and Specifications* document that 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`
		Read the Certification document that 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`

3	Install the Oracle 11.1.1 database and any required patches.	For more information, see Installing Oracle Database.
4	Install Oracle WebLogic Server, and create a Middleware Home.	For more information, see Installing Oracle WebLogic Server 10.3.3 and Creating the Oracle Middleware Home.
5	Run Oracle Fusion Middleware Repository Creation Utility (RCU) to create and load the appropriate schemas for Oracle Identity Management products	For more information, see Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU).
6	Install the Oracle Identity Management 11g software.	For more information, see Installing OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0).
7	For Oracle Identity Manager users only: Install the latest version of Oracle SOA Suite 11*g*.	Install the 11.1.1.2.0 version of Oracle SOA Suite, but do not configure a WebLogic domain for Oracle SOA Suite at this stage. You must configure Oracle SOA Suite after patching Oracle SOA Suite 11.1.1.2.0 to 11.1.1.5.0, which is the latest version of Oracle SOA Suite 11*g*. For more information, see Installing the Latest Version of Oracle SOA Suite (Oracle Identity Manager Users Only).
8	Run the Oracle Fusion Middleware Configuration Wizard to configure your Oracle Identity Management products in a new or existing WebLogic domain.	For more information, see the following chapters: ■ Configuring Oracle Identity Navigator ■ Configuring Oracle Identity Manager ■ Configuring Oracle Access Manager ■ Configuring Oracle Adaptive Access Manager ■ Configuring Oracle Authorization Policy Manager
9	Start the servers.	For more information, see Starting the Stack.
10	For Oracle Identity Manager users only: Run the Oracle Identity Manager Configuration Wizard to configure Oracle Identity Manager Server, Design Console, or Remote Manager. Note that you should run the Oracle Identity Manager Server after completing this configuration.	For more information, see the following topics: ■ Configuring OIM Server ■ Configuring OIM Design Console ■ Configuring OIM Remote Manager

Oracle Identity Management components will not start running after installing them using the Oracle Identity Management 11*g* Installer. For information about starting the components after installation, see the Getting Started topics in specific chapters in this guide.

The following figure illustrates the process of installing the Oracle Identity Management 11*g* software components (the suite containing OIM, OAM, OAAM, OAPM, and OIN).

Figure 2–1 Oracle Identity Management Installation and Configuration Workflow

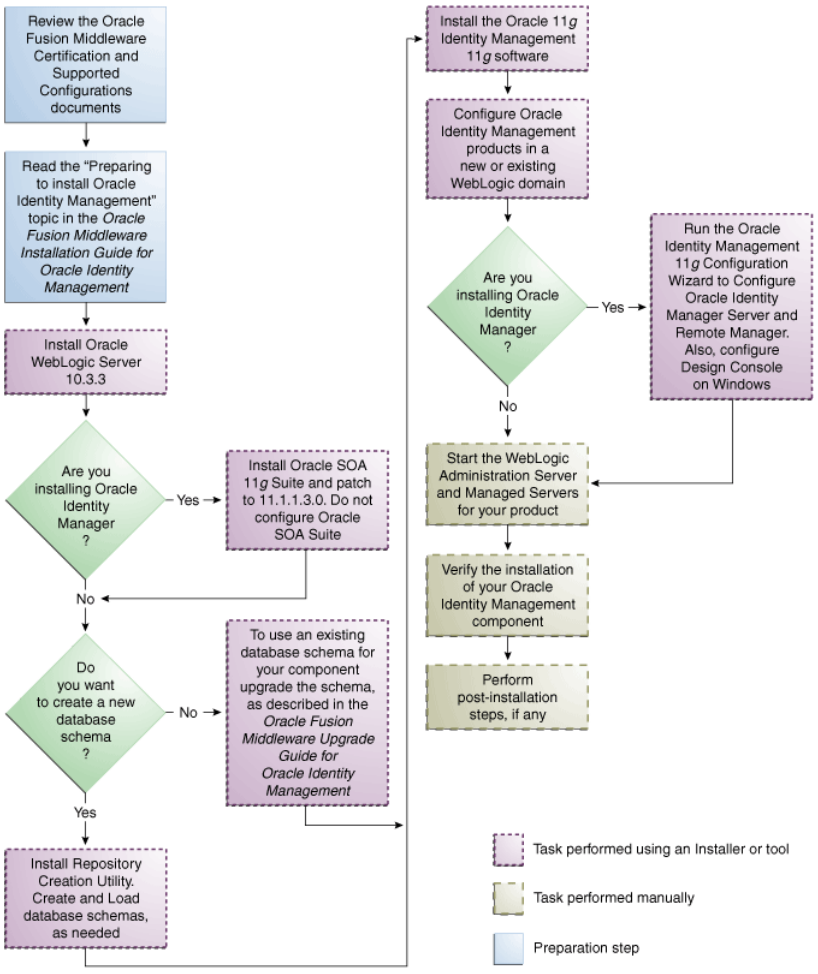


Table 2–3 lists the Installers and tools used to install and configure Oracle Identity Management 11*g* components at different stages of the installation process.

Table 2–3 Installation and Configuration Tools

Task	Tool
Install Oracle WebLogic Server	Oracle WebLogic Server Installer For more information, see Installing Oracle WebLogic Server 10.3.3 and Creating the Oracle Middleware Home.

Table 2–3 (Cont.) Installation and Configuration Tools

Task	Tool
Install Oracle SOA 11*g* Suite	Oracle SOA 11*g* Suite Installer For more information, see Installing the Latest Version of Oracle SOA Suite (Oracle Identity Manager Users Only).
Create and load database schema	Oracle Fusion Middleware Repository Creation Utility (RCU) For more information, see Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU).
Upgrade your existing database schema	Oracle Fusion Middleware 11*g* Upgrade Assistant For more information, see the guide *Oracle Fusion Middleware Upgrade Guide for Oracle Identity Management*.
Install the Oracle Identity Management 11*g* software	Oracle Identity Management 11*g* Installer For more information, see Installing OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0).
Create or extend a WebLogic administration domain	Oracle Fusion Middleware Configuration Wizard For more information, see Screens in Oracle Fusion Middleware Configuration Wizard.
Install and configure Oracle Identity Manager Server, Design Console, and Remote Manager	Oracle Identity Manager 11*g* Configuration Wizard For more information, see Configuring OIM Server, Design Console, and Remote Manager.

2.3.2 Prerequisite Checks Performed by the Oracle Identity Management Installer

The Oracle Identity Management 11*g* Release 1 (11.1.1.3.0) Installer ensures that your machine has a certified version of the operating system, the correct software packages (service packs), and sufficient physical memory to install the Oracle Identity Management applications on your machine.

On Windows operating systems, the Installer verifies the operating system version, service pack, and physical memory (at least 1024 MB).

On UNIX operating systems, the Installer verifies the operating system version, operating system packages, kernel parameters, glibc version, and physical memory (at least 1024 MB).

2.3.3 Understanding Oracle WebLogic Server Administration Domain Options

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

This section describes each domain option for installing Oracle Identity Management components:

- Create a New Domain
- Extend an Existing Domain

See: The "Understanding Oracle WebLogic Server Domains" chapter in the *Oracle Fusion Middleware Understanding Domain Configuration for Oracle WebLogic Server* guide for more information about Oracle WebLogic Server administration domains.

2.3.3.1 Create a New Domain

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

2.3.3.2 Extend an Existing Domain

Select the **Extend an existing WebLogic domain** option on the Welcome screen in the Oracle Fusion Middleware Configuration Wizard to add Oracle Identity Management components in an existing Oracle WebLogic Server administration domain. When you add Oracle Identity Management components using this option, they are essentially "joining" an existing domain.

For more information, see Understanding Domain Extension Scenarios.

2.3.4 Additional Configuration Using the Oracle Identity Manager 11*g* Configuration Wizard

Read this section only if you are installing Oracle Identity Manager. After you install Oracle Identity Manager by using the Oracle Identity Management 11*g* Installer software, you can encrypt secure data in Oracle Identity Manager schema, create keystores, and so on. You can configure such elements by using the Oracle Identity Manager 11*g* Release 1 (11.1.1) Configuration Wizard, which is included with the release media.

On UNIX operating systems, to start the Oracle Identity Manager 11*g* Release 1 (11.1.1) Configuration Wizard, run the `<IAMSUITE_IDM_HOME>/bin/config.sh` script. On Windows operating systems, run the `<IAMSUITE_IDM_HOME>\bin\config.bat` script. Note that `IAMSUITE_IDM_HOME` refers to your IDM_Home directory that contains Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Authorization Policy Manager, and Oracle Identity Navigator.

2.3.5 Additional 11*g* Release 1 (11.1.1.3.0) Deployment Information

This topic describes additional sources for 11*g* Release 1 (11.1.1.3.0) deployment information, including documentation on the following subjects:

- Upgrading to 11g Release 1 (11.1.1.3.0)
- Installing 11g Release 1 (11.1.1.3.0) for High Availability

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

2.3.5.1 Upgrading to 11*g* Release 1 (11.1.1.3.0)

This guide does not explain how to upgrade previous versions of Oracle Identity Management components to 11*g* Release 1 (11.1.1.3.0). To upgrade an Oracle Identity Management component:

From Release 10*g* to 11*g* Release 1 (11.1.1.3.0), refer to:

- *Oracle Fusion Middleware Upgrade Planning Guide*

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

2.3.5.2 Installing 11*g* Release 1 (11.1.1.3.0) for High Availability

This guide does not explain how to install Oracle Identity Management components in High Availability (HA) configurations. To install an Oracle Identity Management component in a High Availability configuration, refer to the following documents:

- *Oracle Fusion Middleware High Availability Guide*
- *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management*

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

2.3.6 Silent Installation

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

For more information, see Performing a Silent Installation.

2.3.7 Installing Components on Separate Systems

You can install Oracle Fusion Middleware instances on separate systems. You can also distribute Oracle Fusion Middleware components over multiple systems, which is especially useful for Oracle Identity Management components. You might want to distribute components to improve performance, security, scalability, and availability of Oracle Identity Management services.

The following are two (of many) examples of Oracle Identity Management deployments that benefit from distributing components over multiple systems:

- Oracle Identity Manager Server on one system, and Oracle Identity Manager Design Console on a different system.
- Oracle Identity Management components use an Oracle Database to contain the Oracle Metadata Repository. The Oracle Identity Management components and the Oracle Database are installed on separate systems.

> **Note:** If you install Oracle Identity Management components on a separate system from the database containing the Oracle Metadata Repository, the Oracle Identity Management components will need network access to the repository.

2.3.8 Screens in Oracle Fusion Middleware Configuration Wizard

The Oracle Fusion Middleware Configuration Wizard displays screens based on your domain configuration options. You can use the Oracle Fusion Middleware Configuration Wizard in the following scenarios:

- Creation of a new WebLogic administration domain, which involves the configuration of Administration Server parameters, server start mode, and so on.
- Configuration of an existing domain to support Oracle Identity Management components by extending the domain.

See: The "Customizing the Domain Environment" chapter in the *Oracle Fusion Middleware Creating Domains Using the Configuration Wizard* guide for more information about configuring your domain.

The appendix WebLogic Domain Configuration Screens in this guide for screens in the Oracle Fusion Middleware Configuration Wizard.

2.3.9 Understanding the State of Oracle Identity Management Components After Installation

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

- Default SSL Configurations
- Default Passwords

2.3.9.1 Default SSL Configurations

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

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

2.3.9.2 Default Passwords

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

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

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

3

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 (11.1.1.5.0)
- Before Installing OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0)

> **Note:** For information about prerequisites for installing the 11*g* (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 11.1.1.5.0, see Before Installing OID, OVD, ODSM, ODIP, and OIF (11.1.1.5.0).
>
> 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).

3.1 Before Installing OID, OVD, ODSM, ODIP, and OIF (11.1.1.5.0)

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)
- Optional Environment-Specific Preparation

3.1.1 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).

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

3.1.2 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 `access-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.

3.1.3 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`*

3.1.4 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

Note: Ensure that the following database parameters are set:

- `'aq_tm_processes' >= 1`
- `'db_cache_size' >= '150994944'`
- `'java_pool_size'>= '125829120'`
- `'shared_pool_size' >= '183500800'`

If you are installing a new database, be sure to configure your database to use AL32UTF8 character set encoding. If your database does not use the AL32UTF8 character set, you will see the following warning when running RCU: "The database you are connecting is with non-AL32UTF8 character set. Oracle strongly recommends using AL32UTF8 as the database character set." You can ignore this warning and continue using RCU.

3.1.5 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.

  If you are installing Oracle Internet Directory and your database is not configured as per the requirements in the fusion middleware requirements and prerequisites doc, you would see the following warnings: "Recommended value for Database initialization parameter processes is 500. Choose YES to continue or NO to go back to the same screen and specify different database details." To fix this one can click No and apply the requisite configuration mentioned in the fusion middleware requirements and prerequisites doc - section 8 Repository Creation Utility (RCU) Requirements which can be accessed from the following link:

  http://download.oracle.com/docs/html/E18558_01/fusion_requirements.htm#CHDJGECA

- 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 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 x86 and Windows x86 platforms. 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 the Oracle Identity Management component you are installing—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.

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

3.1.6 Optional Environment-Specific Preparation

This topic describes optional environment-specific tasks you may want to perform before installing Oracle Identity Management 11*g* Release 1 (11.1.1.5.0). This topic includes the following sections:

- Using Symbolic Links
- Installing Oracle Identity Management on DHCP Hosts
- Installing Oracle Identity Management on a Multihomed System

Note: If the environment variable LD_ASSUME_KERNEL is set, it needs to be unset.

3.1.6.1 Using Symbolic Links

If you want to install Oracle Identity Management using symbolic links, you must create them before installation. For example, you could create symbolic links for the installation by executing the following commands:

```
prompt> mkdir /home/basedir
prompt> ln -s /home/basedir /home/linkdir
```

Then, when you run the Installer to install Oracle Identity Management, you can specify /home/linkdir as the Oracle Home.

After installation, you cannot create symbolic links to the Oracle Home. Also, you cannot move the Oracle Home to a different location and create a symbolic link to the original Oracle Home.

3.1.6.2 Installing Oracle Identity Management on DHCP Hosts

If you plan to install Oracle Identity Management components on a DHCP server, you must ensure the Installer can resolve host names. This may require editing the /etc/hosts file on UNIX systems, and installing a loopback adapter on Windows systems. The following information provides general examples, you should alter these examples to make them specific to your environment.

On UNIX systems:

Configure the host to resolve host names to the loopback IP address by modifying the /etc/hosts file to contain the following entries. Replace the *variables* with the appropriate host and domain names:

```
127.0.0.1 hostname.domainname hostname
127.0.0.1 localhost.localdomain localhost
```

Confirm the host name resolves to the loopback IP address by executing the following command:

```
ping hostname.domainname
```

On Windows systems:

Install a loopback adapter on the DHCP host and assign it a non routable IP address.

After installing the adapter, add a line to the %SYSTEMROOT%\system32\drivers\etc\hosts file immediately after the localhost line and using the following format, where *IP_address* represents the local IP address of the loopback adapter:

```
IP_address   hostname.domainname   hostname
```

3.1.6.3 Installing Oracle Identity Management on a Multihomed System

You can install Oracle Identity Management components on a multihomed system. A multihomed system is associated with multiple IP addresses, typically achieved by having multiple network cards on the system. Each IP address is associated with a host name and you can create aliases for each host name.

The Installer retrieves the fully qualified domain name from the first entry in /etc/hosts file on UNIX, or the %SYSTEMROOT%\system32\drivers\etc\hosts file on Windows. For example, if your file looks like the following, the Installer retrieves myhost1.mycompany.com for configuration:

```
127.0.0.1 localhost.localdomain localhost
10.222.333.444 myhost1.mycompany.com myhost1
20.222.333.444 devhost2.mycompany.com devhost2
```

For specific network configuration of a system component, refer to the individual component's documentation listed in "Related Documents"for more information.

3.2 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)

3.2.1 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 (11.1.1.3.0).

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/fusion-certification-100350.html`

3.2.2 System Requirements

This topic describes the system requirements for installing Oracle Identity Management 11*g* Release 1 (11.1.1.3.0) and includes the following sections:

- Most Recent Information
- Installer Startup Requirements
- Memory Requirements

3.2.2.1 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`

3.2.2.2 Installer Startup Requirements

When you start the Installer, it checks for the requirements listed in Table 3–1. The Installer will notify you if any requirements are not met.

Table 3–1 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

3.2.2.3 Memory Requirements

Table 3–2 lists the minimum memory requirements to install Oracle Identity Management 11*g* Release 1 (11.1.1.3.0):

Table 3–2 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 (11.1.1.3.0) deployment depends on which components, or combination of components, you install.

3.2.3 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.

3.2.4 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*.

3.2.5 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.

For more information, see "Install Oracle WebLogic Server" in *Oracle Fusion Middleware Installation Planning Guide*.

In addition, see *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server* for complete information about installing Oracle WebLogic Server.

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.

3.2.6 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 3–3 lists the databases requirements for RCU at the time of publication:

Table 3–3 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: 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.

3.2.6.1 Oracle Database 11.1.0.7 Patch Requirements for Oracle Identity Manager

To identify the patches required for Oracle Identity Manager 11.1.1.3.0 configurations that use Oracle Database 11.1.0.7, refer to the Oracle Identity Manager section of the 11*g* Release 1 (11.1.1.3.0) Oracle Fusion Middleware Release Notes.

3.2.7 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 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 OAAM Partition Schema Reference.

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

- For Oracle 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.

3.2.8 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*.

3.2.9 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.

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

3.2.9.1 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* (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*.

3.2.9.2 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.

3.2.9.3 Installing the Latest Version of Oracle SOA Suite

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

Follow the instructions in Table 3–4 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 3–4 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.

Table 3–4 (Cont.) Installation Flow for Install Only Option

No.	Screen	Description and Action Required
4	Specify Security Updates Screen	Provide your E-mail address to be informed of the latest product issues. Click **Next** to continue.
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.

3.2.9.4 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*.

4

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 (11.1.1.5.0)
- Common Installation Tasks for OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0)

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

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

- Installing OID, OVD, ODSM, ODIP, and OIF (11.1.1.5.0)
- Installing OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0)

For complete information about configuring Oracle Identity Management software, see the individual component specific chapters in the following links:

- Installing and Configuring OID, OVD, ODSM, ODIP, and OIF (11.1.1.5.0)
- Installing and Configuring OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0)

4.1 Common Installation Tasks for OID, OVD, ODSM, ODIP, and OIF (11.1.1.5.0)

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

4.1.1 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 (11.1.1.5.0) 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 11.1.1.5.0, see Patching the Oracle Identity Management 11.1.1.2.0 to 11.1.1.5.0.

4.1.2 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 4–1 to configure the inventory directory information:

Table 4–1 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>
```

4.1.3 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

4.1.3.1 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.

4.1.3.2 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.

4.1.3.3 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.

4.1.3.4 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 and runtime components 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.

4.1.3.5 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.

4.1.4 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.

- $*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 OPMN.

4.1.5 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. Refer to Appendix C, "Performing Silent Installations" for more information.

     > **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 as described in "Executing the oracleRoot.sh Script on UNIX Platforms" and continue to the Configuration Progress screen.

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.

4.1.6 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.

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 4–1 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 4–1 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 Appendix B, "Starting or Stopping the Oracle 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.

4.1.7 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

4.2 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
- Optional: Updating the WebLogic Administrator Server User Name in Oracle Enterprise Manager Fusion Middleware Control (OIM Only)

4.2.1 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_17/jre`

   Windows: `<full path to the setup.exe directory>\ setup.exe -jreLoc <Middleware Home>\jrockit_160_17\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_17` 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_17`, then launch the installer from the command prompt as follows:
   >
   > `D:\setup.exe -jreLoc D:\oracle\Middleware\jrockit_160_17\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, continue by referring to Installing and Configuring OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0).

4.2.2 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.cmd` 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.

After starting the Oracle Fusion Middleware Configuration Wizard, configure Oracle Identity Management products, as described in the following links:

- Configuring Oracle Identity Navigator
- Configuring Oracle Identity Manager
- Configuring Oracle Access Manager
- Configuring Oracle Adaptive Access Manager
- OAM and OAAM Joint Domain Configuration Scenarios
- Configuring Oracle Authorization Policy Manager

4.2.3 List of Executable Files

Table 4–2 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 4–2 Executable Files

File	Description
`iamsuite.zip` After you extract the contents of the `iamsuite.zip` file to a directory, you can see the executable file `runInstaller` (for UNIX) or `setup.exe` (for Windows) in the `Disk1` directory.	Oracle Identity Management 11*g* Release 1 (11.1.1.3.0) 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` After you extract the contents of the `soa.zip` file to a directory, you can see the executable file `runInstaller` (for UNIX) or `setup.exe` (for Windows) in the `Disk1` directory.	Oracle SOA Suite 11*g* Release 1 (11.1.1.2.0) Installer

Table 4–2 (Cont.) Executable Files

File	Description
`soa_patchset.zip` After you extract the contents of the `soa_patchset.zip` file to a directory, you can see the executable file `runInstaller` (for UNIX) or `setup.exe` (for Windows) in the `Disk1` directory.	Oracle SOA Suite 11*g* Release 1 (11.1.1.3.0) Patch Set Installer
`webtier.zip` After you extract the contents of the `webtier.zip` file to a directory, you can see the executable file `runInstaller` (for UNIX) or `setup.exe` (for Windows) in the `Disk1` directory.	Oracle Web Tier 11*g* Release 1 (11.1.1) Installer
`webgate.zip` After you extract the contents of the `webgate.zip` file to a directory, you can see the executable file `runInstaller` (for UNIX) or `setup.exe` (for Windows) in the `Disk1` directory.	Oracle HTTP Server 11*g* Webgate for Oracle Access Manager Installer
`rcuHome.zip` After you extract the contents of the `rcuHome.zip` file to a directory, you can see the executable file `rcu` in the `BIN` directory.	Oracle Fusion Middleware Repository Creation Utility (RCU)

4.2.4 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

4.2.4.1 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*.

4.2.4.2 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.

4.2.4.3 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*.

4.2.4.4 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)*.

4.2.4.5 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*.

4.2.5 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.

4.2.6 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 Performing a Silent Installation for more information.

     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.

4.2.7 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

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

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

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

1. Ensure that the Oracle Identity Manager Managed server is up and running.
2. Log in to Oracle Enterprise Manager Fusion Middleware Control using your WebLogic Server administrator credentials.
3. Click **Identity and Access** > **oim** > **oim(11.1.1.2.0)**. Right-click and select **System MBean Browser**. The System MBean Browser page is displayed.
4. Under Application Defined MBeans, select `oracle.iam` > `Server:oim_server1` > `Application: oim` > `XMLConfig` > `config` > `>XMLConfig.SOAConfig` > `SOAConfig`.
5. View the attribute username. By default, the value of the attribute is weblogic. Change this value to your WebLogic administrator user name.
6. Click **Apply**. Exit Oracle Enterprise Manager Fusion Middleware Control.
7. On the command line, use the `cd` command to move from your present working directory to the `Oracle_IDM2/common/bin` directory. **Oracle_IDM2** is the example IDM_Home directory for Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Authorization Policy Manager, and Oracle Identity Navigator.
8. Launch the WebLogic Scripting Tool (WLST) interface as follows:

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

   On Windows: Run `wlst.cmd`.

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

   ```
   connect()
   ```

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

   a. Run the `deleteCred` WLST command:

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

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

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

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

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

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

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

Part II

Installing and Configuring OID, OVD, ODSM, ODIP, and OIF (11.1.1.5.0)

Part II provides information about configuring the following Oracle Identity Management products:

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

Additionally, Part II provides information about installing Oracle Single Sign-On and Oracle Delegated Administration Services against Oracle Internet Directory.

Part II contains the following chapters:

5

Installing OID, OVD, ODSM, ODIP, and OIF (11.1.1.5.0)

This chapter includes the following topics:

- Installing OID, OVD, ODSM, ODIP, and OIF (11.1.1.5.0)
- Configuring OID, OVD, ODSM, ODIP, and OIF (11.1.1.5.0)

5.1 Installing OID, OVD, ODSM, ODIP, and OIF (11.1.1.5.0)

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

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

1. Obtaining Oracle Fusion Middleware 11g Softwares
2. Installing Oracle WebLogic Server 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 11.1.1.5.0

> **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.

5.1.1 Obtaining Oracle Fusion Middleware 11*g* Softwares

- 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 (10.3.5)
  - Oracle Identity Management 11*g* Release 1 (11.1.1.2.0)
  - Oracle Identity Management 11*g* Release 1 (11.1.1.5.0)

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 11.1.1.5.0 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 11.1.1.5.0 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* (10.3.5).
- For complete information about patching your Oracle Fusion Middleware 11*g* to the latest release, refer to the *Oracle Fusion Middleware Patching Guide*.

5.1.2 Installing Oracle WebLogic Server 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 *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server* for complete information about installing Oracle WebLogic Server.

Notes:

- If you are installing Oracle Internet Directory without an Oracle WebLogic administration domain, you do not need to install Oracle WebLogic.
- The same user who 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.

5.1.3 Installing the 11.1.1.2.0 Version of Oracle Identity Management Software

Follow the instructions in Table 5–1 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 5–1 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.

Table 5–1 (Cont.) Installation Flow for Install Only Option

No.	Screen	Description and Action Required
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 11.1.1.5.0

5.1.4 Patching the Oracle Identity Management 11.1.1.2.0 to 11.1.1.5.0

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 11.1.1.5.0

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* (10.3.5) on your machine.

   Note: If you are installing Oracle Internet Directory 11*g* Release 1 (11.1.1.5.0) without an Oracle WebLogic administration domain, you do not need to install Oracle WebLogic.

2. Ensure that Oracle Identity Management 11*g* Release 1 (11.1.1.5.0) Patch Set Installer (`ofm_idm_win_11.1.1.5.0_32_disk1_1of1.zip` (for **Windows**) or `ofm_idm_linux_11.1.1.5.0_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_11.1.1.5.0_32_disk1_1of1.zip` (for **Windows**) or `ofm_idm_linux_11.1.1.5.0_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 (11.1.1.5.0) 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 (11.1.1.5.0). You are now ready to configure your Oracle Identity Management 11*g* Release 1 (11.1.1.5.0) components:

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

5.2 Configuring OID, OVD, ODSM, ODIP, and OIF (11.1.1.5.0)

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:

- Only OID in an Existing WebLogic Domain
- Only OID Without a WebLogic Domain
- OID with ODSM and Fusion Middleware Control in a New WebLogic Domain
- OID with ODIP, ODSM, and Fusion Middleware Control in a New WebLogic Domain
- OVD with ODSM and Fusion Middleware Control in a New WebLogic Domain
- Only OVD in an Existing WebLogic Domain
- Only OVD Without a WebLogic Domain
- Performing Basic OIF Configurations
- Performing Advanced OIF Configurations
- ODIP with Fusion Middleware Control in a New WebLogic Domain
- Only ODIP in an Existing WebLogic Domain
- Configuring ODIP when OID is Running in SSL Mode 2 - Server Only Authentication

6

Configuring Oracle Internet Directory

This chapter explains how to configure Oracle Internet Directory (OID). You can configure Oracle Internet Directory after installing the software, as described in Installation Roadmap and Installing OID, OVD, ODSM, ODIP, and OIF (11.1.1.5.0).

This chapter discusses the following topics:

- OID with ODSM and Fusion Middleware Control in a New WebLogic Domain
- OID with ODIP, ODSM, and Fusion Middleware Control in a New WebLogic Domain
- OID and OVD with ODSM in a New WebLogic Domain
- Only OID in an Existing WebLogic Domain
- Only OID Without a WebLogic Domain
- Verifying OID Installation
- Getting Started with OID After Installation

Table 6–1 Oracle Internet Directory Configuration Scenarios

Scenario	Description
OID with ODSM and Fusion Middleware Control in a New WebLogic Domain	The configuration described in this topic is appropriate for environments that have *all* of the following conditions: ■ You want to manage Oracle Internet Directory using Fusion Middleware Control. ■ You want Oracle Internet Directory to be in a WebLogic administration domain. ■ There is no WebLogic Administration Server managing other 11*g* Release 1 (11.1.1) Oracle Directory Services components. ■ You want to install Oracle Internet Directory and a WebLogic Administration Server colocated on the same host.
OID with ODIP, ODSM, and Fusion Middleware Control in a New WebLogic Domain	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 11*g* Release 1 (11.1.1) Oracle Directory Services components.

Table 6–1 (Cont.) Oracle Internet Directory Configuration Scenarios

Scenario	Description
OID and OVD with ODSM in a New WebLogic Domain	The configuration described in this topic is appropriate for environments that have the following conditions: ■ A new WebLogic Administration Server is necessary to manage Oracle Internet Directory and Oracle Virtual Directory components. ■ You want to install Oracle Internet Directory and Oracle Virtual Directory together in the same WebLogic domain, which can be extended at a later time to add new Oracle Identity Management components.
Only OID in an Existing WebLogic Domain	The configuration described in this topic is appropriate for environments that have *both* of the following conditions: ■ A WebLogic Administration Server is available to manage 11*g* Release 1 (11.1.1) Oracle Directory Services components and you want Oracle Internet Directory to join that domain. ■ You want to install Oracle Internet Directory separately from the WebLogic Administration Server.
Only OID Without a WebLogic Domain	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.

6.1 OID with ODSM and Fusion Middleware Control in a New WebLogic Domain

This topic describes how to configure Oracle Internet Directory (OID) 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

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

6.1.2 Components Deployed

Performing the configuration in this section deploys the following components:

- WebLogic Administration Server
- Oracle Internet Directory
- Oracle Directory Services Manager
- Fusion Middleware Control

6.1.3 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.

6.1.4 Procedure

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

1. Ensure that Oracle Internet Directory is installed, as described in Installation Roadmap and Installing OID, OVD, ODSM, ODIP, and OIF (11.1.1.5.0).
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**. 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 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 of *hostname*:*port*:*servicename*. For Oracle Real Application Clusters (RAC), the connection string must be in the form of *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 of *hostname*:*port*:*servicename*. For Oracle Real Application Clusters (RAC), the connection string must be in the form of *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.

Note: If you are using Oracle Database 11*g* Release 2 (11.2) or higher version, the database user should be only 'SYS'.

---

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.

6.2 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

6.2.1 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 11*g* Release 1 (11.1.1) Oracle Directory Services components.

6.2.2 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

6.2.3 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.

6.2.4 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, Oracle Directory Integration Platform, and Oracle Directory Services Manager are installed, as described in Installation Roadmap and Installing OID, OVD, ODSM, ODIP, and OIF (11.1.1.5.0).
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 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 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 of *hostname*:*port*:*servicename*. For Oracle Real Application Clusters (RAC), the connection string must be in the form of *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 of *hostname*:*port*:*servicename*. For Oracle Real Application Clusters (RAC), the connection string must be in the form of *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.

Note: If you are using Oracle Database 11*g* Release 2 (11.2) or higher version, the database user should be only 'SYS'.

---

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.

6.3 OID and OVD with ODSM in a New WebLogic Domain

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

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure

6.3.1 Appropriate Deployment Environment

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

- A new WebLogic Administration Server is necessary to manage Oracle Internet Directory and Oracle Virtual Directory components.
- You want to install Oracle Internet Directory and Oracle Virtual Directory together in the same WebLogic domain, which can be extended at a later time to add new Oracle Identity Management components.

6.3.2 Components Deployed

Performing the configuration in this section deploys the following:

- WebLogic Administration Server
- Oracle Internet Directory
- Oracle Virtual Directory
- WebLogic Managed Server
- Oracle Directory Services Manager
- Fusion Middleware Control

6.3.3 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.

6.3.4 Procedure

Perform the following steps to configure Oracle Internet Directory and Oracle Virtual Directory in a new domain:

1. Ensure that Oracle Internet Directory and Oracle Virtual Directory are installed, as described in Installation Roadmap and Installing OID, OVD, ODSM, ODIP, and OIF (11.1.1.5.0).
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 Virtual Directory**. 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 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 Specify Schema Database screen is displayed.

9. 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 of *hostname*:*port*:*servicename*. For Oracle Real Application Clusters (RAC), the connection string must be in the form of *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 of *hostname*:*port*:*servicename*. For Oracle Real Application Clusters (RAC), the connection string must be in the form of *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.

Note: If you are using Oracle Database 11*g* Release 2 (11.2) or higher version, the database user should be only 'SYS'.

---

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.

10. 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.

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

6.4 Only OID in an Existing WebLogic Domain

This topic describes how to configure only Oracle Internet Directory (OID) in an existing WebLogic administration domain. It includes the following sections:

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure

6.4.1 Appropriate Deployment Environment

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

- A WebLogic Administration Server is available to manage 11*g* Release 1 (11.1.1) Oracle Directory Services components and you want Oracle Internet Directory to join that domain.
- You want to install Oracle Internet Directory separately from the WebLogic Administration Server.

6.4.2 Components Deployed

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

6.4.3 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.

6.4.4 Procedure

Perform the following steps to configure only Oracle Internet Directory in an existing domain:

1. Ensure that Oracle Internet Directory is installed, as described in Installation Roadmap and Installing OID, OVD, ODSM, ODIP, and OIF (11.1.1.5.0).
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 **Extend Existing Domain** and enter the following information:
   - Enter the name of the host that contains the domain in the Host Name field.
   - Enter the Oracle WebLogic Server listen port in the Port field.
   - Enter the user name for the domain in the User Name field.
   - Enter the password for the domain user in the User Password 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.

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

   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 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 of *hostname*:*port*:*servicename*. For Oracle Real Application Clusters (RAC), the connection string must be in the form of *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 of *hostname*:*port*:*servicename*. For Oracle Real Application Clusters (RAC), the connection string must be in the form of *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.

Note: If you are using Oracle Database 11*g* Release 2 (11.2) or higher version, the database user should be only 'SYS'.

---

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.

6.5 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

6.5.1 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 and Oracle Directory Services Manager using Fusion Middleware Control.

6.5.2 Components Deployed

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

6.5.3 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.

6.5.4 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 Installation Roadmap and Installing OID, OVD, ODSM, ODIP, and OIF (11.1.1.5.0).

   Note: 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. On the Select Domain screen, select **Configure without a Domain** 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 of *hostname*:*port*:*servicename*. For Oracle Real Application Clusters (RAC), the connection string must be in the form of *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 of *hostname*:*port*:*servicename*. For Oracle Real Application Clusters (RAC), the connection string must be in the form of *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.

Note: If you are using Oracle Database 11*g* Release 2 (11.2) or higher version, the database user should be only 'SYS'.

---

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.

6.6 Verifying OID Installation

Verify the Oracle Internet Directory (OID) 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 Oracle Internet Directory 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
  ```

6.7 Getting Started with OID After Installation

After installing Oracle Internet Directory (OID), refer to the "Getting Started with Oracle Internet Directory" chapter in the *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*.

7

Configuring Oracle Virtual Directory

This chapter explains how to configure Oracle Virtual Directory (OVD). You must configure Oracle Virtual Directory after installing the softfware, as described in Installation Roadmap and Installing OID, OVD, ODSM, ODIP, and OIF (11.1.1.5.0).

This chapter discusses the following topics:

- OVD with ODSM and Fusion Middleware Control in a New WebLogic Domain
- Only OVD in an Existing WebLogic Domain
- Only OVD Without a WebLogic Domain
- Verifying OVD
- Getting Started with OVD After Installation

7.1 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

7.1.1 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 11*g* 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.

7.1.2 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

7.1.3 Dependencies

The configuration in this section depends on Oracle WebLogic Server.

7.1.4 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 is installed, as described in Installation Roadmap and Installing OID, OVD, ODSM, ODIP, and OIF (11.1.1.5.0).
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".

7.2 Only OVD in an Existing WebLogic Domain

This topic describes how to configure only Oracle Virtual Directory (OVD) in an existing WebLogic administration domain. It includes the following sections:

7.2.1 Appropriate Deployment Environment

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

- A WebLogic Administration Server is available to manage 11*g* Release 1 (11.1.1) Oracle Directory Services components and you want Oracle Virtual Directory to join that domain.
- You want to install Oracle Virtual Directory separately from the WebLogic Administration Server.

7.2.2 Components Deployed

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

7.2.3 Dependencies

The configuration in this section depends on Oracle WebLogic Server.

7.2.4 Procedure

Perform the following steps to configure only Oracle Virtual Directory in an existing domain:

1. Ensure that Oracle Virtual Directory is installed, as described in Installation Roadmap and Installing OID, OVD, ODSM, ODIP, and OIF (11.1.1.5.0).
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 **Extend Existing Domain** and enter the following information:
   a. Enter the name of the host that contains the domain in the Host Name field.
   b. Enter the Oracle WebLogic Server listen port in the Port field.
   c. Enter the user name for the domain in the User Name field.
   d. Enter the password for the domain user in the User Password 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.

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

   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**. 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".

7.3 Only OVD Without a WebLogic Domain

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

7.3.1 Appropriate Deployment Environment

Perform the configuration in this topic if you want to register Oracle Virtual Directory with a remote WebLogic Administration Server for management purposes, but you do not want to install Oracle WebLogic Server locally.

Note: To manage Oracle Virtual Directory using Fusion Middleware Control in this environment, you must register Oracle Virtual Directory with the remote WebLogic Administration Server after installation.

7.3.2 Components Deployed

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

7.3.3 Dependencies

The configuration in this section depends on Oracle WebLogic Server.

7.3.4 Procedure

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

1. Ensure that Oracle Virtual Directory is installed, as described in Installation Roadmap and Installing OID, OVD, ODSM, ODIP, and OIF (11.1.1.5.0).

   Note: 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. Select only **Oracle Virtual 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 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.
10. Execute the following command to register Oracle Virtual Directory with the WebLogic Administration Server. Registering with the WebLogic Administration

Server allows you to manage Oracle Virtual Directory using Fusion Middleware Control.

```
$ORACLE_INSTANCE/bin/opmnctl registerinstance
 -adminHost HOSTNAME
 -adminPort WEBLOGIC_PORT
 -adminUsername WEBLOGIC_ADMIN_USERNAME
```

Note: You will be prompted for the WebLogic administrator's user name and password.

For example:

```
$ORACLE_INSTANCE/bin/opmnctl registerinstance \
 -adminHost myhost \
 -adminPort 7001 \
 -adminUsername weblogic \
```

Note: The default administrative port on the WebLogic Administration Server is 7001.

7.4 Verifying OVD

Verify the Oracle Virtual Directory (OVD) installation by:

- Executing the `$ORACLE_INSTANCE/bin/opmnctl status -l` command.
- Executing the `$ORACLE_HOME/bin/ldapbind` command on the Oracle Virtual Directory non-SSL and SSL ports.

7.5 Getting Started with OVD After Installation

After installing Oracle Virtual Directory (OVD), refer to the "Getting Started with Administering Oracle Virtual Directory" chapter in the *Oracle Fusion Middleware Administrator's Guide for Oracle Virtual Directory*.

8

Configuring Oracle Directory Integration Platform

This chapter explains how to configure Oracle Directory Integration Platform (ODIP). You must configure Oracle Directory Integration Platform after installing the software, as described in Installation Roadmap and Installing OID, OVD, ODSM, ODIP, and OIF (11.1.1.5.0).

This chapter discusses the following topics:

- ODIP with Fusion Middleware Control in a New WebLogic Domain
- Only ODIP in an Existing WebLogic Domain
- Configuring ODIP when OID is Running in SSL Mode 2 - Server Only Authentication
- Verifying ODIP
- Getting Started with ODIP After Installation

8.1 ODIP with Fusion Middleware Control in a New WebLogic Domain

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

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure

8.1.1 Appropriate Deployment Environment

The configuration described in this topic is appropriate if there is no WebLogic Administration Server managing other 11*g* Release 1 (11.1.1) Oracle Directory Services components and Oracle Internet Directory is installed without a domain.

8.1.2 Components Deployed

Performing the configuration in this section deploys the following components:

- WebLogic Managed Server
- Oracle Directory Integration Platform

- WebLogic Administration Server
- Fusion Middleware Control

8.1.3 Dependencies

The configuration in this section depends on the following:

- Oracle WebLogic Server
- Oracle Internet Directory
- Oracle Database for Oracle Internet Directory
- *Identity Management - Oracle Internet Directory* schema existing in the Oracle Internet Directory database.

8.1.4 Procedure

Perform the following steps to configure Oracle Directory Integration Platform with Fusion Middleware Control in a new domain:

1. Ensure that Oracle Directory Integration Platform is installed, as described in Installation Roadmap and Installing OID, OVD, ODSM, ODIP, and OIF (11.1.1.5.0).
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 Directory Integration Platform**. The Fusion Middleware Control management component is 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 OID Details screen appears.

8. Identify the Oracle Internet Directory for Oracle Directory Integration Platform by entering the following information:
   - Hostname: Enter the hostname or IP address of the Oracle Internet Directory host.
   - Port: Enter the Oracle Internet Directory LDAP SSL port.
   - User Name: Enter the user name of the Oracle Internet Directory Administrator.
   - Password: Enter the password for the user name Oracle Directory Integration Platform will use to connect to Oracle Internet Directory.

   Click **Next**. The Specify Schema Database screen appears.
9. Enter the following information about the Oracle Internet Directory schema:
   - Connect String: Enter the database connection information. The connection string must be in the form of *hostname*:*port*:*servicename*. For Oracle Real Application Clusters (RAC), the connection string must be in the form of *hostname1*:*port1*:*instance1*^*hostname2*:*port2*:*instance2*@*servicename*.
   - Password: Enter the password for the ODSSM schema in the Password field.

   Click **Next**. The Installation Summary screen appears.
10. Complete the installation by performing all the steps in "Completing an Installation".

8.2 Only ODIP in an Existing WebLogic Domain

This topic describes how to configure only Oracle Directory Integration Platform (ODIP) in an existing WebLogic administration domain. It includes the following sections:

8.2.1 Appropriate Deployment Environment

The configuration described in this topic is appropriate for the following environments:

An environment that has the following condition:

- A WebLogic Administration Server is managing an 11*g* Release 1 (11.1.1) Oracle Internet Directory component and you want Oracle Directory Integration Platform to join that domain.

An environment that has the following condition:

- A WebLogic Administration Server is managing other 11*g* Release 1 (11.1.1) Oracle Directory Services—but not Oracle Internet Directory, which is installed without a domain.

8.2.2 Components Deployed

Performing the configuration in this section deploys the following components:

- WebLogic Managed Server
- Oracle Directory Integration Platform

8.2.3 Dependencies

The configuration in this section depends on the following:

- Oracle WebLogic Server
- Oracle Internet Directory
- Oracle Database for Oracle Internet Directory
- *Identity Management - Oracle Internet Directory* schema existing in the Oracle Internet Directory database.

8.2.4 Procedure

Perform the following steps to configure only Oracle Directory Integration Platform in an existing domain:

1. Ensure that Oracle Directory Integration Platform is installed, as described in Installation Roadmap and Installing OID, OVD, ODSM, ODIP, and OIF (11.1.1.5.0).
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 **Extend Existing Domain** and enter the following information:
   - Enter the name of the host that contains the domain in the Host Name field.
   - Enter the Oracle WebLogic Server listen port in the Port field.
   - Enter the user name for the domain in the User Name field.
   - Enter the password for the domain user in the User Password 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.

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

   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 Directory Integration Platform**. 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 OID Details screen appears.
8. Identify the Oracle Internet Directory for Oracle Directory Integration Platform by entering the following information:
   - Hostname: Enter the hostname or IP address of the Oracle Internet Directory host.
   - Port: Enter the Oracle Internet Directory LDAP SSL port.
   - User Name: Enter the user name of the Oracle Internet Directory Administrator.
   - Password: Enter the password for the user name Oracle Directory Integration Platform will use to connect to Oracle Internet Directory.

   Click **Next**. The Specify Schema Database screen appears.
9. Enter the following information about the Oracle Internet Directory schema:
   - Connect String: Enter the database connection information. The connection string must be in the form of *hostname*:*port*:*servicename*. For Oracle Real Application Clusters (RAC), the connection string must be in the form of *hostname1*:*port1*:*instance1*^*hostname2*:*port2*:*instance2*@*servicename*.
   - Password: Enter the password for the ODSSM schema in the Password field.

   Click **Next**. The Installation Summary screen appears.
10. Complete the installation by performing all the steps in Completing an Installation.

8.3 Configuring ODIP when OID is Running in SSL Mode 2 - Server Only Authentication

You cannot install and configure Oracle Directory Integration Platform (ODIP) 11*g* Release 1 (11.1.1) when Oracle Internet Directory (OID) is already installed and running in SSL Mode 2 - Server Only Authentication.

If Oracle Internet Directory is already installed and running in SSL Mode 2 - Server Only Authentication, you must perform the following steps to configure Oracle Directory Integration Platform 11*g* Release 1 (11.1.1):

1. Configure Oracle Internet Directory to temporarily run in SSL Mode 1 - No Authentication.

   Refer to the "Configuring Secure Sockets Layer (SSL)" chapter in the *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory* for complete information.

2. Install Oracle Directory Integration Platform, as described in Installation Roadmap and Installing OID, OVD, ODSM, ODIP, and OIF (11.1.1.5.0).

3. Configure Oracle Internet Directory to run in SSL Mode 2 - Server Only Authentication again. Refer to the "Configuring Secure Sockets Layer (SSL)" chapter in the *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*.

4. Configure Oracle Directory Integration Platform to run in SSL Mode 2 by referring to the following sections in the *Oracle Fusion Middleware Integration Guide for Oracle Identity Management*:

   - Configuring Oracle Directory Integration Platform for SSL Mode 2 - Server Only Authentication
   - Managing the SSL Certificates of Oracle Internet Directory and Connected Directories

8.4 Verifying ODIP

Verify the Oracle Directory Integration Platform (ODIP) installation using the `dipStatus` command, which is 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.

8.5 Getting Started with ODIP After Installation

After you install Oracle Directory Integration Platform (ODIP), no additional configuration is needed. The next step is to create synchronization profiles.

The *Oracle Fusion Middleware Integration Guide for Oracle Identity Management* explains how to manage Oracle Directory Integration Platform. For information about creating synchronization profiles using Oracle Enterprise Manager Fusion Middleware Control Console, refer to the "Managing Synchronization Profiles Using Fusion Middleware Control" section in that guide.

9

Configuring Oracle Directory Services Manager

This chapter explains how to configure Oracle Directory Services Manager (ODSM). You must configure Oracle Directory Services Manager after installing the software, as described in Installation Roadmap and Installing OID, OVD, ODSM, ODIP, and OIF (11.1.1.5.0).

This chapter discusses the following topics:

- Only ODSM in a New WebLogic Domain
- Only ODSM in an Existing WebLogic Domain
- Verifying ODSM
- Getting Started with ODSM After Installation

9.1 Only ODSM in a New WebLogic Domain

This topic describes how to configure only Oracle Directory Services Manager (ODSM) in a new WebLogic administration domain. It includes the following sections:

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure

9.1.1 Appropriate Deployment Environment

The configuration described in this topic is appropriate if Oracle Internet Directory was installed without a domain and you want to manage it using Oracle Directory Services Manager.

9.1.2 Components Deployed

Performing the configuration in this section deploys the following components:

- WebLogic Managed Server
- Oracle Directory Services Manager
- WebLogic Administration Server
- Fusion Middleware Control

9.1.3 Dependencies

The configuration in this section depends on Oracle WebLogic Server.

9.1.4 Procedure

Perform the following steps to configure only Oracle Directory Services Manager in a new domain:

1. Ensure that Oracle Directory Services Manager is installed, as described in Installation Roadmap and Installing OID, OVD, ODSM, ODIP, and OIF (11.1.1.5.0).
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 Directory Services Manager**. The Fusion Middleware Control management component is 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 Installation Summary screen appears.
8. Complete the installation by performing all the steps in Completing an Installation.

9.2 Only ODSM in an Existing WebLogic Domain

This topic describes how to configure only Oracle Directory Services Manager (ODSM) in an existing WebLogic administration domain. It includes the following sections:

9.2.1 Appropriate Deployment Environment

The configuration described in this topic is appropriate if you want to deploy an additional Oracle Directory Services Manager component in an existing domain.

9.2.2 Components Deployed

Performing the configuration in this section deploys the following components:

- WebLogic Managed Server
- Oracle Directory Services Manager

9.2.3 Dependencies

The configuration in this section depends on Oracle WebLogic Server.

9.2.4 Procedure

Perform the following steps to configure only Oracle Directory Services Manager in an existing domain:

1. Ensure that Oracle Directory Services Manager is installed, as described in Installation Roadmap and Installing OID, OVD, ODSM, ODIP, and OIF (11.1.1.5.0).
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 **Extend Existing Domain** and enter the following information:
   a. Enter the name of the host that contains the domain in the Host Name field.
   b. Enter the Oracle WebLogic Server listen port in the Port field.
   c. Enter the user name for the domain in the User Name field.
   d. Enter the password for the domain user in the User Password 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".

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

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 Directory Services Manager**. 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 Installation Summary screen appears.
8. Complete the installation by performing all the steps in Completing an Installation.

9.3 Verifying ODSM

To verify the Oracle Directory Services Manager (ODSM) 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 of the Managed Server through the Oracle WebLogic Administration Console. After logging in to the console, expand Environment on the left navigation pane. Click Servers. The Summary of Servers page is displayed. The port for the Oracle Directory Services Manager (ODSM) Managed Server is displayed on this page.

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 Oracle Internet Directory or Oracle Virtual Directory from Oracle Directory Services Manager without the appropriate credentials.

9.4 Getting Started with ODSM After Installation

After you install Oracle Directory Services Manager (ODSM), no additional configuration is needed. The next step is to log in to Oracle Internet Directory or Oracle Virtual Directory. The process for logging in to both directory servers is the same. Information about logging in to both Oracle Internet Directory and Oracle Virtual Directory provided below so you can learn more about Oracle Directory Services Manager in the context of each directory server.

- For information about logging in to Oracle Internet Directory from Oracle Directory Services Manager, refer to the "Logging in to the Directory Server from Oracle Directory Services Manager" section in the *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*.
- For information about logging in to Oracle Virtual Directory from Oracle Directory Services Manager, refer to the "Logging in to the Directory Server from Oracle Directory Services Manager" section in the *Oracle Fusion Middleware Administrator's Guide for Oracle Virtual Directory*.

10

Configuring Oracle Identity Federation

This chapter explains how to configure Oracle Identity Federation (OIF). You must configure Oracle Identity Federation after installing the software, as described in Installation Roadmap and Installing OID, OVD, ODSM, ODIP, and OIF (11.1.1.5.0).

This chapter discusses the following topics:

- Using the Information in This Chapter
- Understanding OIF Deployments
- Understanding OIF Basic and Advanced Deployments
- Configuring Oracle HTTP Server for OIF
- Performing Basic OIF Configurations
- Performing Advanced OIF Configurations
- Advanced Example: Configuring OIF with OID in a New WebLogic Domain for LDAP Authentication, User Store, and Federation Store
- Advanced Example: Configuring OIF in a New or Existing WebLogic Domain with RDBMS Data Stores
- Verifying OIF
- Getting Started with OIF After Installation

10.1 Using the Information in This Chapter

Oracle Identity Federation deployments vary greatly. As described in the following topics, there are several components, and several options for those components, that comprise an Oracle Identity Federation deployment.

Use this chapter as a starting point for your Oracle Identity Federation deployment, as it does not describe every possible installation and configuration. You should also use the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*, which provides additional and detailed deployment information, to supplement the information in this chapter.

10.2 Understanding OIF Deployments

When you configure Oracle Identity Federation (OIF) 11*g* Release 1 (11.1.1), a WebLogic Managed Server is created and the Oracle Identity Federation J2EE application is installed on it. If you configure Oracle Identity Federation in a new Oracle WebLogic Server administration domain by selecting the Create Domain option, the Fusion Middleware Control management component is also deployed.

Oracle Identity Federation functionality depends on several components and modules. You can integrate and configure these components and modules during or after the Oracle Identity Federation installation.

The following is a list and brief description of some of the components and modules that determine Oracle Identity Federation functionality. Refer to the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation* for complete information.

- **Authentication Engine**: The module that challenges users when they log in.
- **User Data Store**: The repository containing the identity information of the users the Oracle Identity Federation system authenticates.
- **Federation Data Store**: The repository containing federated user account linking data.
- **Service Provider (SP) Integration Engine**: The module that creates a local authenticated session for the user based on a received federated Single Sign-On (SSO) token.
- **User Session Store and Message Store**: The repository containing transient runtime session state data and protocol messages.
- **Configuration Data Store**: The repository containing Oracle Identity Federation configuration data.

10.3 Understanding OIF Basic and Advanced Deployments

There are two types of Oracle Identity Federation (OIF) 11*g* Release 1 (11.1.1) deployments: Basic and Advanced. This topic describes both types of deployments and includes the following sections:

- Basic Deployment
- Advanced Deployments

10.3.1 Basic Deployment

The Basic deployment includes Oracle Identity Federation with minimum functionality enabled and the following configuration:

- No User Data Store
- No Federation Store
- JAAS Authentication Engine
- Test Service Provider (SP) Engine
- Memory Session Data Store
- Memory Message Data Store
- XML file system Configuration Store

10.3.2 Advanced Deployments

The Advanced deployments allows you to choose between different types of data stores and authentication engines. The following is a list and description of the types of data stores and authentication engines you can choose during an Advanced installation:

Authentication Engine

- JAAS: Delegates authentication to the application server.
- LDAP: Uses form login and LDAP bind with credentials supplied by user to authenticate against LDAP repository.

User Data Store

- None: No User Data Store. Typically used with Custom or JAAS Authentication Engines, environments without user attributes, or Windows CardSpace.
- LDAP: Typical configuration that stores user data in an LDAP repository.
- RDBMS: Uses database tables with user names (and optionally user attributes) in columns.

Federation Data Store

- None: No Federation Data Store. Typically used when there are no persistent account linking records. No Federation Data Store is also an alternative to using name identifiers, such as e-mail address, X.509 DN, Kerberos, or Windows Name Identifier.
- LDAP: Stores federation in an LDAP repository. Commonly deployed when the User Data Store is also LDAP.
- RDBMS: Stores federation in a relational database repository. Commonly deployed when the User Data Store is also RDBMS.
- XML: Stores federation data in an XML file system. Commonly used for testing purposes.

User Session Store and Message Store

- Memory: Stores transient runtime session state data and protocol messages in in-memory tables. Commonly used for single instance deployments. Memory provides better performance than the RDBMS User Session Store, but increases runtime memory requirements.
- RDBMS: Stores transient runtime session state data and protocol messages in a relational database. Recommended for High Availability cluster environments.

> **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.

Configuration Data Store

- File System: Stores Oracle Identity Federation configuration data on the local file system. Commonly used in single-instance and testing environments.
- RDBMS: Stores Oracle Identity Federation configuration data in a relational database. Commonly used in High Availability environments or single-instances with failover redundancy.

10.4 Configuring Oracle HTTP Server for OIF

When you install Oracle Identity Federation (OIF), Oracle HTTP Server also gets installed. 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.

To configure the Oracle HTTP Server so that the Oracle Identity Federation application can be accessed through Oracle HTTP Server ports, you can:

- Ensure that Oracle Identity Federation is installed, as described in Installation Roadmap and Installing OID, OVD, ODSM, ODIP, and OIF (11.1.1.5.0).
- 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.
- On the Configure Components screen, select Oracle HTTP Server and Oracle Identity Federation.

> **See:** 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 about integrating Oracle Identity Federation and Oracle HTTP Server.

10.5 Performing Basic OIF Configurations

This topic describes how to perform a Basic Oracle Identity Federation (OIF) configuration. It includes the following sections:

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure

10.5.1 Appropriate Deployment Environment

The Basic Oracle Identity Federation configuration is appropriate for:

- Creating a base to gradually build complex implementations upon after installation
- Deploying test environments
- Deploying small, self-contained configurations

10.5.2 Components Deployed

Performing the Basic Oracle Identity Federation configuration deploys the following components:

If you install Oracle Identity Federation in a new domain:

- WebLogic Managed Server
- Oracle Identity Federation
- WebLogic Administration Server
- Fusion Middleware Control
- *Optionally*, Oracle HTTP Server

If you install Oracle Identity Federation in an existing domain:

- WebLogic Managed Server
- Oracle Identity Federation

- *Optionally*, Oracle HTTP Server

10.5.3 Dependencies

The Basic Oracle Identity Federation configuration depends on Oracle WebLogic Server.

10.5.4 Procedure

Perform the following steps to deploy a Basic Oracle Identity Federation configuration:

1. Ensure that Oracle Identity Federation is installed, as described in Installation Roadmap and Installing OID, OVD, ODSM, ODIP, and OIF (11.1.1.5.0).
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, choose whether to configure Oracle Identity Federation in a new or existing domain:

To configure Oracle Identity Federation in a new domain:

a. Select **Create New Domain**.

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

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

Enter the user password again in the Confirm Password field.

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

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

Continue the installation by going to step 4 now.

To configure Oracle Identity Federation in an existing domain:

a. Select **Extend Existing Domain**.

b. Enter the name of the host that contains the domain in the Host Name field.

c. Enter the listen port for the WebLogic Administration Server in the Port field.

d. Enter the user name for the domain in the User Name field.

e. Enter the password for the domain user in the User Password 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".

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

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 Identity Federation**—and *optionally*, **Oracle HTTP Server**. Refer to "Configuring Oracle HTTP Server for OIF" on page 10-3 for information about configuring these two components simultaneously.

   If you are installing Oracle Identity Federation in a new domain, the Fusion Middleware Control management component is automatically selected for 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 Select Oracle Identity Federation Configuration Type screen appears.
8. Select **Basic** and click **Next**. The Specify OIF Details screen appears.
9. 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 Installation Summary screen appears.
10. Complete the installation by performing all the steps in Completing an Installation.

10.6 Performing Advanced OIF Configurations

This topic generally describes how to perform an Advanced Oracle Identity Federation (OIF) configuration. Refer to the next two topics in this chapter for information on performing specific Advanced Oracle Identity Federation configurations.

This topic includes the following sections:

10.6.1 Appropriate Deployment Environment

The Advanced Oracle Identity Federation configuration provides a fast and simplified method for deploying Oracle Identity Federation with its vital components integrated and configured.

10.6.2 Components Deployed

Performing the Advanced Oracle Identity Federation configuration deploys the following components:

If you configure Oracle Identity Federation in a new domain:

- WebLogic Managed Server
- Oracle Identity Federation
- WebLogic Administration Server
- Fusion Middleware Control
- *Optionally*, Oracle HTTP Server

If you configure Oracle Identity Federation in an existing domain:

- WebLogic Managed Server
- Oracle Identity Federation
- *Optionally*, Oracle HTTP Server

10.6.3 Dependencies

The Advanced Oracle Identity Federation configuration depends on the following components:

- Oracle WebLogic Server
- Oracle Database, if using RDBMS for User Store, Federation Store, Session Store, Message Store, or Configuration Store.
- New *Identity Management - Oracle Identity Federation* schema existing in the database, if using RDBMS for Federation Store, Session Store, Message Store, or Configuration Store.
- Database table for storing user dative using RDBMS for User Store
- LDAP repository, if using LDAP for Authentication, User Store, or Federation Store.

10.6.4 Procedure

Perform the following steps to deploy an Advanced Oracle Identity Federation configuration:

1. Decide if you want to use RDBMS for User Store, Federation Store, 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.

   Note: The schema is not required for RDBMS User Stores.

2. Decide if you want to use an LDAP repository for Authentication, User Store, or Federation Store. If you do, you must install the LDAP repository before you can install Oracle Identity Federation.
3. Ensure that Oracle Identity Federation is installed, as described in Installation Roadmap and Installing OID, OVD, ODSM, ODIP, and OIF (11.1.1.5.0).
4. 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.
5. On the Select Domain screen, choose whether to install Oracle Identity Federation in a new or existing domain:

To configure Oracle Identity Federation in a new domain:

   a. Select **Create New Domain**.
   b. Enter the user name for the new domain in the User Name field.
   c. Enter the user password for the new domain in the User Password field.
   d. Enter the user password again in the Confirm Password field.
   e. Enter a name for the new domain in the Domain Name field.
   f. Click **Next**. The Specify Installation Location screen appears.

   Continue the installation by going to step 6 now.

To configure Oracle Identity Federation in an existing domain:

   a. Select **Extend Existing Domain**.
   b. Enter the name of the host that contains the domain in the Host Name field.
   c. Enter the listen port for the WebLogic Administration Server in the Port field.
   d. Enter the user name for the domain in the User Name field.
   e. Enter the password for the domain user in the User Password field.
   f. Click **Next**. The Specify Installation Location screen appears.

6. Identify the Homes, Instances, and the WebLogic Server directory by referring to Identifying Installation Directories.

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

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

7. 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.
8. Select **Oracle Identity Federation**—and *optionally*, **Oracle HTTP Server**. Refer to "Configuring Oracle HTTP Server for OIF" on page 10-3 for information about configuring these two components simultaneously.

   If you are installing Oracle Identity Federation in a new domain, the Fusion Middleware Control management component is automatically selected for installation.

   Ensure no other components are selected and click **Next**. The Configure Ports screen appears.
9. 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 Select Oracle Identity Federation Configuration Type screen appears.
10. Select **Advanced** and click **Next**. The Specify OIF Details screen appears.
11. 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.

12. 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.

The screens that appear next depend on the options you selected for the configuration items on the Select OIF Advanced Flow Attributes screen. The following information describes all possible screens that may appear. This information about all possible screens that may appear is not presented in a linear sequence and your installation may not encounter all of the screens. Enter information for the appropriate screens and proceed to step 13.

If you selected LDAP for Authentication Type, the Specify Authentication LDAP Details screen will appear. Enter the following information:

- LDAP Type: Select the appropriate LDAP repository.
- LDAP URL: Enter the URL connection string for the LDAP repository in the form: *protocol://hostname:port*

> **Note:** If you selected Microsoft Active Directory for the LDAP Type, you must specify an SSL LDAP URL, that is, ldaps://*hostname*:*port*.

- LDAP Bind DN: Enter the bind DN for the LDAP repository.
- LDAP Password: Enter the password for the bind DN.
- User Credential ID Attribute: Enter the LDAP attribute Oracle Identity Federation will use to authenticate users. For example, if you enter **mail** and the value of the mail attribute for a user is jane.doe@domain.com, then Jane Doe must enter **jane.doe.@domain.com** when challenged. Values for the LDAP attribute you identify for User Credential ID Attribute must be unique for all users.
- User Unique ID Attribute: Enter the LDAP attribute that will uniquely identify users to Oracle Identity Federation. The value you enter must be identical to the value you enter for the User Data Store's User ID Attribute parameter. For example, if you enter mail for User Unique ID Attribute and you configure the User Data Store's User ID Attribute parameter with a value of EmailAddress, then the value of mail in the authentication engine repository must equal the value of EmailAddress in the User Data Store. Values for the LDAP attribute you identify for User Unique ID Attribute must be unique for all users.
- Person Object Class: Enter the LDAP object class that represents a user in the LDAP repository. For example: inetOrgPerson for Oracle Internet Directory and Sun Java System Directory Server, and user for Microsoft Active Directory.
- Base DN: Enter the root DN that searches will start from.

If you selected LDAP for User Store, the Specify LDAP Attributes for User Data Store screen will appear. Enter the following information:

- LDAP Type: Select the appropriate LDAP repository.

- LDAP URL: Enter the URL connection string for the LDAP repository in the form: *protocol://hostname:port*

> **Note:** If you selected Microsoft Active Directory for the LDAP Type, you must specify an SSL LDAP URL, that is, ldaps://*hostname*:*port*.

- LDAP Bind DN: Enter the bind DN for the LDAP repository.
- LDAP Password: Enter the password for the bind DN.
- User Description Attribute: Enter the readable LDAP attribute that will identify the owner of a federation record. For example: uid for Oracle Internet Directory and Sun Java System Directory Server, and sAMAccountName for Microsoft Active Directory.
- User ID Attribute: Enter the LDAP attribute that will uniquely identify the user during authentication. For example: uid for Oracle Internet Directory and Sun Java System Directory Server, and sAMAccountName for Microsoft Active Directory.
- Person Object Class: Enter the LDAP object class that represents a user in the LDAP repository. For example: inetOrgPerson for Oracle Internet Directory and Sun Java System Directory Server, and user for Microsoft Active Directory.
- Base DN: Enter the root DN that searches will start from.

If you selected RDBMS for User Store, the Specify User Store Database Details screen will appear. Enter the following information:

- 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 database username.
- Password: Enter the password for the database user.
- Login Table: Enter the name of the table that will store user data. The value you enter must be a valid table name, and the values you enter for User ID Attribute and User Description Attribute must be valid column names in the table you identify.
- User ID Attribute: Enter the name of the table column to use for the Oracle Identity Federation user ID. The value you enter must be a valid column name in the table you identified for the Login Table parameter.
- User Description Attribute: Enter the name of the table column to use for the user description. The value you enter must be a valid column name in the table you identified for the Login Table parameter.

If you selected LDAP for Federation Store, the Specify LDAP Attributes for Federation Data Store screen will appear. Enter the following information:

- LDAP Type: Select the appropriate LDAP repository.
- LDAP URL: Enter the URL connection string for the LDAP repository in the form: *protocol://hostname:port*

Note: If you selected Microsoft Active Directory for the LDAP Type, you must specify an SSL LDAP URL, that is, ldaps://*hostname*:*port*.

- LDAP Bind DN: Enter the bind DN for the LDAP repository.
- LDAP Password: Enter the password for the bind DN.
- User Federation Record Context: Enter the location of the container where you want Oracle Identity Federation to store federation records. If the container you identify does not exist, it will be created at runtime. However, if you identify cn=example,dc=test,dc=com as the User Federation Record Context, dc=test,dc=com must exist in the LDAP repository.
- LDAP Container Object Class: *Optional*. Enter the object class for the container that stores federation records. If this field is empty, the default value of applicationProcess is used.
- Active Directory Domain: Appears only if you select Microsoft Active Directory for the LDAP Type. Enter the name of the Microsoft Active Directory domain.

If you selected RDBMS for Federation Store, the Specify Federation Store Database Details screen will appear. Enter the following information:

- 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.

If you selected RDBMS for User Session Store, Message Store, or Configuration Store, the Specify Transient Store Database Details screen will appear. Enter the following information:

- 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.

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

10.7 Advanced Example: Configuring 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

10.7.1 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.

10.7.2 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

10.7.3 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.

10.7.4 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 is installed, as described in Installation Roadmap and Installing OID, OVD, ODSM, ODIP, and OIF (11.1.1.5.0).
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**. Refer to "Configuring Oracle HTTP Server for OIF" on page 10-3 for information about configuring Oracle HTTP Server with Oracle Identity Federation.

   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 of *hostname*:*port*:*servicename*. For Oracle Real Application Clusters (RAC), the connection string must be in the form of *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.

10.8 Advanced Example: Configuring OIF in a New or Existing WebLogic Domain with RDBMS Data Stores

This topic describes how to configure Oracle Identity Federation (OIF) in a new or existing WebLogic administration domain with RDBMS data stores. It includes the following sections:

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure

10.8.1 Appropriate Deployment Environment

Perform the configuration in this topic to quickly deploy Oracle Identity Federation with RDBMS User Store, Federation Store, Session Store, Message Store, and Configuration Store.

10.8.2 Components Deployed

Performing the configuration in this section deploys the following components:

If you configure Oracle Identity Federation in a new domain:

- WebLogic Administration Server
- Fusion Middleware Control
- WebLogic Managed Server
- Oracle Identity Federation
- *Optionally*, Oracle HTTP Server

If you configure Oracle Identity Federation in an existing domain:

- WebLogic Managed Server
- Oracle Identity Federation
- *Optionally*, Oracle HTTP Server

10.8.3 Dependencies

The configuration in this section depends on the following:

- Oracle WebLogic Server
- Oracle Database for User Store, Federation Store, Session Store, Message Store, and Configuration Store.

- New *Identity Management - Oracle Identity Federation* schema existing in the database for Federation Store, Session Store, Message Store, and Configuration Store.
- Table for storing user data in the User Store database.
- LDAP repository, if using LDAP for Authentication.

10.8.4 Procedure

Perform the following steps to configure Oracle Identity Federation in a new or existing domain with RDBMS User Store, Federation Store, User Session Store, Message Store, and Configuration Store:

1. Install the database(s) for the RDBMS User Store, Federation Store, User Session Store, Message Store, and Configuration Store. Refer to Installing Oracle Database for more information.
2. Create the *Identity Management - Oracle Identity Federation* schema in the database(s). Refer to Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU) for more information.
3. Decide if you want to use an LDAP repository for Authentication. If you do, you must install the LDAP repository before you can install Oracle Identity Federation.
4. Ensure that Oracle Identity Federation is installed, as described in Installation Roadmap and Installing OID, OVD, ODSM, ODIP, and OIF (11.1.1.5.0).
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, choose whether to install Oracle Identity Federation in a new or existing domain:

To configure Oracle Identity Federation in a new domain:

a. Select **Create New Domain**.
b. Enter the user name for the new domain in the User Name field.
c. Enter the user password for the new domain in the User Password field.
d. Enter the user password again in the Confirm Password field.
e. Enter a name for the new domain in the Domain Name field.
f. Click **Next**. The Specify Installation Location screen appears.
g. Continue the installation by going to step 7 now.

To install Oracle Identity Federation in an existing domain:

a. Select **Extend Existing Domain**.
b. Enter the name of the host that contains the domain in the Host Name field.
c. Enter the listen port for the WebLogic Administration Server in the Port field.
d. Enter the user name for the domain in the User Name field.
e. Enter the password for the domain user in the User Password field.
f. Click **Next**. The Specify Installation Location screen appears.

7. Identify the Homes, Instances, and the WebLogic Server directory by referring to Identifying Installation Directories.

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

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 Identity Federation**—and *optionally*, **Oracle HTTP Server**. Refer to "Configuring Oracle HTTP Server for OIF" on page 10-3 for information about configuring these two components simultaneously.

   If you are installing Oracle Identity Federation in a new domain, the Fusion Middleware Control management component is automatically selected for 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 Select Oracle Identity Federation Configuration Type screen appears.
11. Select **Advanced** and click **Next**. The Specify OIF Details screen appears.
12. 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.

13. Select the following and click **Next**:
    - Authentication Type: **JAAS** or **LDAP**
      - Select JAAS to delegate authentication to the application server.
      - Select LDAP to authenticate against an LDAP repository.
    - User Store: **RDBMS**
    - Federation Store: **RDBMS**
    - User Session Store: **RDBMS**
    - Message Store: **RDBMS**
    - Configuration Store: **RDBMS**

    Note: The screen that appears next depends on what you selected for Authentication:

    - If you selected LDAP for Authentication Type, the Specify Authentication LDAP Details screen appears. Continue you installation by going to step 14 now.
    - If you selected JAAS for Authentication Type, the Specify User Store Database Details screen appears. Continue you installation by going to step 15 now.

    ---

14. Enter the following information on the Specify Authentication LDAP Details screen to identify the LDAP repository that will perform authentication:
    - LDAP Type: Select the appropriate LDAP repository.
    - LDAP URL: Enter the URL connection string for the LDAP repository in the form: *protocol://hostname:port*

      Note: If you selected Microsoft Active Directory for the LDAP Type, you must specify an SSL LDAP URL, that is, ldaps://*hostname*:*port*.

    - LDAP Bind DN: Enter the bind DN for the LDAP repository.
    - LDAP Password: Enter the password for the bind DN.
    - User Credential ID Attribute: Enter the LDAP attribute Oracle Identity Federation will use to authenticate users. For example, if you enter **mail** and the value of the mail attribute for a user is jane.doe@domain.com, then Jane Doe must enter **jane.doe.@domain.com** when challenged. Values for the LDAP attribute you identify for User Credential ID Attribute must be unique for all users.
    - User Unique ID Attribute: Enter the LDAP attribute that will uniquely identify users to Oracle Identity Federation. The value you enter must be identical to the value you enter for the User Data Store's User ID Attribute parameter. For example, if you enter mail for User Unique ID Attribute and you configure the User Data Store's User ID Attribute parameter with a value of EmailAddress, then the value of mail in the authentication engine repository must equal the value of EmailAddress in the User Data Store. Values for the LDAP attribute you identify for User Unique ID Attribute must be unique for all users.

- Person Object Class: Enter the LDAP object class that represents a user in the LDAP repository. For example: inetOrgPerson for Oracle Internet Directory and Sun Java System Directory Server, and user for Microsoft Active Directory.
- Base DN: Enter the root DN that searches will start from.

Click **Next**. The Specify User Store Database Details screen appears.

15. Enter the following information to identify the database that will store user data:
    - 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 database username.
    - Password: Enter the password for the database user.
    - Login Table: Enter the name of the table that will store user data. The value you enter must be a valid table name, and the values you enter for User ID Attribute and User Description Attribute must be valid column names in the table you identify.
    - User ID Attribute: Enter the name of the table column to use for the Oracle Identity Federation user ID. The value you enter must be a valid column name in the table you identified for the Login Table parameter.
    - User Description Attribute: Enter the name of the table column to use for the user description. The value you enter must be a valid column name in the table you identified for the Login Table parameter.

    Click **Next**. The Specify Federation Store Database Details screen appears.
16. Enter the following information to identify the database that will store federated user account linking data:
    - 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.

    Click **Next**. The Specify Transient Store Database screen appears.
17. Enter the following information to identify the database that will store transient runtime session state data, protocol messages, and Oracle Identity Federation configuration data:
    - 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.

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

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

10.9 Verifying OIF

Verify the Oracle Identity Federation (OIF) 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.

10.10 Getting Started with OIF After Installation

After installing Oracle Identity Federation (OIF), refer to the "Common Tasks" section in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*.

11

Installing Oracle Single Sign-On and Oracle Delegated Administration Services Against Oracle Internet Directory

This chapter explains how to install Oracle Single Sign-On and Oracle Delegated Administration Services Release 10*g* (10.1.4.3.0) against Oracle Internet Directory (OID) 11*g* Release 1 (11.1.1).

> **Note:** If you already have Oracle Single Sign-On and Oracle Delegated Administration Services Release 10*g* (10.1.4.3.0) installed against Oracle Internet Directory Release 10g, refer to the *Oracle Fusion Middleware Upgrade Guide for Oracle Identity Management* for information on upgrading to Oracle Internet Directory 11*g* Release 1 (11.1.1).

This chapter includes the following topics:

11.1 Understanding the inspre11.pl Script

You must use the inspre11.pl Perl script when installing Oracle Single Sign-On and Oracle Delegated Administration Services Release 10*g* (10.1.4.3.0) against Oracle Internet Directory 11*g* Release 1 (11.1.1). This topic describes how to use the inspre11.pl script.

The inspre11.pl script is located in the *$ORACLE_HOME*`/ldap/bin/` directory on the host where Oracle Internet Directory 11*g* Release 1 (11.1.1) is installed. Perl is located in the *$ORACLE_HOME*`/perl/bin/` directory.

Before you execute the inspre11.pl script, you must set the following environment variables:

- *ORACLE_INSTANCE* to the Oracle Internet Directory 11*g* Release 1 (11.1.1) Oracle Instance location.
- *ORACLE_HOME* to the Oracle Internet Directory 11*g* Release 1 (11.1.1) Oracle Home location.

The following is the syntax for the inspre11.pl script:

```
$OID11gR1_ORACLE_HOME/perl/bin/perl \
$OID11gR1_ORACLE_HOME/ldap/bin/inspre11.pl OID_HOST OID_PORT {-ssl | -nonssl} \
OID_COMPONENT TNS_CONNECT_STRING ODS_PASSWORD ORCLADMIN_PASSWORD \
{-op1 | -op2 | -op3}
```

The following list defines each of the options for the inspre11.pl script:

OID_HOST
Identifies the host where Oracle Internet Directory 11*g* Release 1 (11.1.1) is installed.

OID_PORT
The SSL or non-SSL Oracle Internet Directory port.

-ssl
Indicates the port identified by *OID_PORT* is the Oracle Internet Directory SSL port.

-nonssl
Indicates the port identified by *OID_PORT* is the Oracle Internet Directory non-SSL port.

OID_COMPONENT
The name of the Oracle Internet Directory component, such as oid1. You can identify the name of the Oracle Internet Directory component using the *$ORACLE_INSTANCE*/bin/opmnctl status command.

TNS_CONNECT_STRING
Represents the Oracle Internet Directory database connect string defined in the *ORACLE_INSTANCE*/config/tnsnames.ora file. The default value is oiddb.

> **Note:** Only use the Oracle Internet Directory database connect string defined in the *ORACLE_INSTANCE*/config/tnsnames.ora file—do not use any other tnsnames.ora file to identify the connect string.

ODS_PASSWORD
The password for the ODS schema.

ORCLADMIN_PASSWORD
The password for the Oracle Internet Directory administrator, which is typically cn=orcladmin.

-op1
Enables anonymous bind and disables entry caching. While the -op1 option does not use the *TNS_CONNECT_STRING* value, you must include it when executing inspre11.pl with the -op1 option.

-op2
Resets the Oracle Internet Directory version to allow you to install Oracle Single Sign-On and Oracle Delegated Administration Services Release 10*g* (10.1.4.3.0). This option also sets the seealso attribute to point to the database identified by the *TNS_CONNECT_STRING* option.

-op3
Sets the Oracle Internet Directory version back to 11*g* Release 1 (11.1.1) and enables entry caching.

11.2 Procedure

Perform the following steps to install Oracle Single Sign-On and Oracle Delegated Administration Services Release 10*g* (10.1.4.3.0) against Oracle Internet Directory 11*g* Release 1 (11.1.1):

1. Install Oracle Internet Directory 11*g* Release 1 (11.1.1). Refer to Chapter 6, "Configuring Oracle Internet Directory" for more information.

2. Execute the inspre11.pl script with -op1. This will enable anonymous bind in Oracle Internet Directory and allow the Oracle OracleAS RepCA to load schema into the database for Oracle Single Sign-On and Oracle Delegated Administration Services. Execute the script as follows:

   ```
   $OID11gR1_ORACLE_HOME/perl/bin/perl \
   $OID11gR1_ORACLE_HOME/ldap/bin/inspre11.pl OID_HOST OID_PORT {-ssl | -nonssl} \
   OID_COMPONENT TNS_CONNECT_STRING ODS_PASSWORD ORCLADMIN_PASSWORD -op1
   ```

   When this command completes successfully, the following message is displayed:

   ```
   'Use RepCA to load SSO and other schemas against DB before
   running -op2'
   ```

   Note: If desired, you can disable anonymous bind in Oracle Internet Directory in the last step of this procedure.

3. Use the OracleAS RepCA Release 10.1.4.3.1 to create and load Oracle Single Sign-On 10.1.4.0.1 schema in the database. You can get OracleAS RepCA 10.1.4.3.1 from the Oracle Technology Network (OTN) Web site:

   http://www.oracle.com/technology/software/products/middleware/htdocs/111110_fmw.html#

   You must use only this specific version of MRCA for installing Oracle Single Sign-On (10.1.4.x) against Oracle Internet Directory 11*g* Release 1 (11.1.1) in an Oracle Fusion Middleware 11*g* deployment. This MRCA cannot be used as a generic replacement for MRCA 10*g* in an Application Server 10*g* deployment because it only carries only a subset of the original MRCA 10*g* schemas to support Oracle Single Sign-On (10.1.4.x) for Oracle Fusion Middleware 11*g* deployment.

Note: While there is no documentation specifically for OracleAS RepCA Release 10.1.4.3.1, you can use the *Oracle Application Server Metadata Repository Creation Assistant User's Guide* for Release 10*g* (10.1.4.0.1) for general information on how to use OracleAS RepCA. Be aware that the database requirements listed in this document do not apply to the OracleAS RepCA Release 10.1.4.3.1.

You can get the *Oracle Application Server Metadata Repository Creation Assistant User's Guide* for Release 10*g* (10.1.4.0.1) from the Oracle Identity Management 10*g* (10.1.4) Documentation Library located on the OTN Web site.

If an already existing Identity Management 10g (10.1.4 or 10.1.2) option is chosen, a separate Oracle Internet Directory 10g and separate Oracle Database may need to be managed along with other options. See the certification, installation and planning guides for more information.

After MRCA 10.1.4.3.1 is installed, you can perform an Identity Management 10g (10.1.4.0.1) installation and choose SSO+DAS only. For information on performing this installation and installing the required patches, see the note that follows **Step 6** in this procedure.

When you run OracleAS RepCA 10.1.4.3.1:

- You must register the Oracle Single Sign-On schema with Oracle Internet Directory using its SSL port. This is required for various Oracle Single Sign-On and Oracle Internet Directory interdependencies.
- You might receive error messages that some database session parameters do not have appropriate values. If you receive these errors, you should reset the parameters identified by OracleAS RepCA, adhering to the minimum values that are given. After you reset the parameters, exit OracleAS RepCA and start it again. If you used SPFILE as the scope in any of the `alter` commands, you may also have to restart the database.
- Only the schema required for Oracle Single Sign-On will be loaded, not all schema.

4. Reset the ODS password to the value that was set when Oracle Internet Directory was installed and restart Oracle Internet Directory. You must reset the password because it was randomized when you loaded the Oracle Single Sign-On 10.1.4.0.1 schema in the database.

   Perform the following steps:

   a. Use SQL*PLUS to connect the database as the SYS user.

   b. Change the ODS password using `alter user ods` identified by *PASSWORD*, where *PASSWORD* represents the ODS schema password before running the OracleAS RepCA.

   c. Set the TNS_ADMIN environment variable to point to the $*ORACLE_INSTANCE*/config directory.

   d. Execute the following command, where *TNS_CONNECT_STRING* represents the Oracle Internet Directory database connect string defined in the *ORACLE_INSTANCE*/config/tnsnames.ora file. You can set the TNS_ADMIN environment variable if you want to use a different location.

```
$OID11gR1_ORACLE_HOME/ldap/bin/oidpasswd \
connect=TNS_CONNECT_STRING create_wallet=true
```

e. Restart Oracle Internet Directory.

5. Execute the inspre11.pl script with -op2, which resets the Oracle Internet Directory version and allows you to install Oracle Single Sign-On and Oracle Delegated Administration Services Release 10*g* (10.1.4.0.1). The -op2 option will also verify the orcldirectoryversion attribute has a value of OID 10.1.4.0.1.

Execute the script as follows:

```
$OID11gR1_ORACLE_HOME/perl/bin/perl \
$OID11gR1_ORACLE_HOME/ldap/bin/inspre11.pl OID_HOST OID_PORT {-ssl | -nonssl} \
OID_COMPONENT TNS_CONNECT_STRING ODS_PASSWORD ORCLADMIN_PASSWORD -op2
```

When this command completes successfully, the following message is displayed:

```
'Install SSO/DAS against 11g OID before running -op3'
```

6. Install Oracle Single Sign-On and Oracle Delegated Administration Services Release 10*g* (10.1.4.0.1) in an *ORACLE_HOME* directory that is different from the *ORACLE_HOME* where you installed Oracle Internet Directory. Do not install Oracle Single Sign-On and Oracle Delegated Administration Services Release 10*g* (10.1.4.0.1) in the same *ORACLE_HOME* where you installed Oracle Internet Directory 11*g* Release 1 (11.1.1).

You can get Oracle Single Sign-On and Oracle Delegated Administration Services Release 10*g* (10.1.4.0.1) from the Oracle Technology Network (OTN) Web site. To access the OTN Web site, go to the following URL:

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

Note: After MRCA 10.1.4.3.1 is installed, you can perform an Identity Management 10*g* (10.1.4.0.1) installation and choose SSO+DAS only, rather than a full Infrastructure. This is available in the 10*g* download location (http://www.oracle.com/technetwork/middleware/ias/downloads/101401-099957.html).

If you are installing Oracle Single Sign-On and Oracle Delegated Administration Services against a Release 11.x database, you must apply **Patch 5649850 for release 10.1.0.5** to the Oracle Single Sign-On *ORACLE_HOME* directory. Patch 5649850 updates the 10.1.0.5 JDBC driver, allowing connectivity to a Release 11.x database. If you are unable to apply this patch due to a prerequisite failure, apply **Patch 6880880 for release 1** before applying patch 5649850.

When you install Oracle Single Sign-On and Oracle Delegated Administration Services, apply patch 5649850 when you are prompted to run the `root.sh` script on UNIX systems. On Windows systems, you should wait for the Configuration Assistant to fail, apply the patch and rerun the Configuration Assistant. Do not shutdown nor restart either OID nor its DB.

You can get **Patch 5649850 for release 10.1.0.5** from My Oracle Support (formerly MetaLink), located at:

http://metalink.oracle.com/

The 10.1.4.3 Patchset (**Patch 7215628**) is then applied to the SSO+DAS home. To apply the 10.1.4.3 Patchset with where a 11.2 database is associated, you must first download **Patch 6265268**, following its readme file. This final 10.1.4.3.0 SSO+DAS home is used in conjunction with the OID 11*g* and MRCA 10.1.4.3.1 previously installed.

---

7. Upgrade Oracle Single Sign-On and Oracle Delegated Administration Services to Release 10*g* (10.1.4.3.0) by applying the Oracle Identity Management 10g (10.1.4.3.0) Patch Set. You can get the Oracle Identity Management 10g (10.1.4.3.0) Patch Set from My Oracle Support (formerly MetaLink) by searching for Bug or **Patch Number 7215628**.

   You can access My Oracle Support (formerly MetaLink) at:

   http://metalink.oracle.com/

8. Execute the inspre11.pl script with -op3, which sets the Oracle Internet Directory version back to 11*g* Release 1 (11.1.1). For example:

   ```
   $OID11gR1_ORACLE_HOME/perl/bin/perl \
   $OID11gR1_ORACLE_HOME/ldap/bin/inspre11.pl OID_HOST OID_PORT {-ssl | -nonssl} \
   OID_COMPONENT TNS_CONNECT_STRING ODS_PASSWORD ORCLADMIN_PASSWORD -op3
   ```

   When this command completes successfully, the following message is displayed:

   ```
   'Finished all actions!'
   ```

9. Executing the inspre11.pl script with -op1 in step 2 enables anonymous bind in Oracle Internet Directory. If desired, you can disable anonymous bind in Oracle Internet Directory by referring to "Managing Anonymous Binds" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*.

11.3 Verifying Oracle Single Sign-On and Oracle Delegated Administration Services

Verify the Oracle Single Sign-On and Oracle Delegated Administration Services Release 10*g* (10.1.4.3.0) installation against Oracle Internet Directory 11*g* Release 1 (11.1.1) by logging in to Oracle Delegated Administration Services. You will be redirected to Oracle Single Sign-On and prompted to log in. If you have access to the Oracle Delegated Administration Services content after logging in to Oracle Single Sign-On, the installation against Oracle Internet Directory 11*g* Release 1 (11.1.1) was successful.

11.4 Getting Started After Installation

The following information describes how to get started after installing Oracle Single Sign-On and Oracle Delegated Administration Services Release 10*g* (10.1.4.3.0) against Oracle Internet Directory 11*g* Release 1 (11.1.1).

11.4.1 Getting Started with Oracle Single Sign-On Release 10g (10.1.4.3.0)

After installing Oracle Single Sign-On Release 10*g* (10.1.4.3.0) against Oracle Internet Directory 11*g* Release 1 (11.1.1) as described in this chapter, refer to the "Basic Administration" chapter in the *Oracle Application Server Single Sign-On Administrator's Guide 10g Release 10.1.4.0.1* available at:

`http://www.oracle.com/technology/documentation/oim1014.html`

11.4.2 Getting Started with Oracle Delegated Administration Services Release 10g (10.1.4.3.0)

After installing Oracle Delegated Administration Services Release 10*g* (10.1.4.3.0) against Oracle Internet Directory 11*g* Release 1 (11.1.1) as described in this chapter, refer to the "Getting Started with Oracle Delegated Administration Services" chapter in the *Oracle Identity Management Guide to Delegated Administration 10g Release 10.1.4.0.1* available at:

`http://www.oracle.com/technology/documentation/oim1014.html`

Part III

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

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

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

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

Part III contains the following chapters:

12

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

This chapter includes the following topics:

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

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

It includes the following sections:

12.1.1 Products Installed

Performing the installation in this section installs the following products:

- Oracle Identity Manager
- Oracle Access Manager
- Oracle Adaptive Access Manager
- Oracle Identity Navigator
- Oracle Authorization Policy Manager

12.1.2 Dependencies

The installation in this section depends on the following:

- Oracle WebLogic Server
- Oracle Database and any required patches
- Oracle SOA Suite 11.1.1.3.0 (required for Oracle Identity Manager only)

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

12.1.3 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 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 Oracle Fusion Middleware Repository Creation Utility (RCU) or if you want to use an existing schema:
   - If you want to create a new schema using the Oracle Fusion Middleware Repository Creation Utility (RCU), 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 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 prompts you to confirm whether you want to proceed with the installation of only Oracle Identity Manager Design Console and Oracle Identity Manager Remote Manager. These two components of Oracle Identity Manager do not require a Middleware Home directory.

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

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

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, Oracle_IDM1, or Oracle_IDM2 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 under your Middleware Home. You must proceed to create a WebLogic Domain, by running the Oracle Fusion Middleware Configuration Wizard. In addition, you must configure the Administration Server settings while creating the domain.

   If you are configuring Oracle Identity Manager (OIM), after configuring a domain, you must run the Oracle Identity Manager Configuration Wizard to configure OIM server, design console, and remote manager.

   For information about configuring Oracle Identity Management products, see the following:

   - Configuring Oracle Identity Navigator
   - Configuring Oracle Identity Manager
   - Configuring Oracle Access Manager
   - Configuring Oracle Adaptive Access Manager
   - OAM and OAAM Joint Domain Configuration Scenarios
   - Configuring Oracle Authorization Policy Manager

   For more information, see Configuring OIM Server, Configuring OIM Design Console, and Configuring OIM Remote Manager.

Note: If you cancel or abort when the installation is in progress, you must manually delete the `<IDM_Home>` directory before you can reinstall the Oracle Identity Management software.

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

12.2 Understanding the Directory Structure After Installation

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

After you install the Oracle Identity Management software, an Oracle Home directory for Oracle Identity Management, such as `Oracle_IDM1`, is created under your Middleware Home. This home directory is also referred to as IDM_Home.

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

12.3 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. In addition, you must configure the Administration Server settings while creating the 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 Understanding Oracle WebLogic Server Administration Domain Options.

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.

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.

12.4 Configuring Oracle Identity Management Products

For information about configuration scenarios for Oracle Identity Management products, including joint-installation scenarios, read the following chapters:

- Configuring Oracle Identity Navigator
- Configuring Oracle Identity Manager
- Configuring Oracle Access Manager
- Configuring Oracle Adaptive Access Manager
- OAM and OAAM Joint Domain Configuration Scenarios
- Configuring Oracle Authorization Policy Manager

13

Understanding Domain Extension Scenarios

This chapter describes the scenarios in which an existing Oracle Identity Management domain can be extended to support new Oracle Identity Management products.

It includes the following topics:

13.1 Overview

When you extend an Oracle Identity Management domain, you are configuring new products in the existing domain to support new Oracle Identity Management products.

For example, you can extend an Oracle Identity Management 11.1.1.3.0 domain to support Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Identity Navigator, or Oracle Authorization Policy Manager. The existing Oracle Identity Management 11.1.1.3.0 domain may contain one or more of the various combinations of Oracle Identity Management products, such as Oracle Internet Directory, Oracle Virtual Directory, Oracle Directory Services Manager, Oracle Identity Federation, or Oracle Directory Integration Platform.

In addition, you can extend an Oracle Identity Management domain that contains any of the various combinations of Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Identity Navigator, and Oracle Authorization Policy Manager.

Note: Note that the existing domain must have been created using the Oracle Identity Management 11*g* Release 1 (11.1.1) Installer and configured using the Oracle Identity Management 11*g* Configuration Wizard. You cannot extend an existing domain for Oracle Identity Management components if the domain was created by another program, such as the Oracle Fusion Middleware 11g Oracle SOA Suite Installer or the Oracle Fusion Middleware Configuration Wizard.

13.2 Important Notes Before You Begin

Before you start installing and configuring Oracle Identity Management products in any of the scenarios discussed in this chapter, keep the following points in mind:

- It is assumed that you are installing Oracle Internet Directory, Oracle Virtual Directory, Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Navigator on the same machine.

  Note: In this chapter, two IDM_Home directories are mentioned in descriptions and procedures. 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 document. You can specify any name for either of your IDM_Home directories. In addition, you can install the two Oracle Identity Management suites (one containing Oracle Internet Directory, Oracle Virtual Directory, Oracle Directory Services Manager, Oracle Directory Integration Platform, and Oracle Identity Federation; another containing Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Authorization Policy Manager, and Oracle Identity Navigator) 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.

  If you have not installed Oracle Internet Directory, Oracle Virtual Directory, Oracle Directory Services Manager, Oracle Directory Integration Platform, or Oracle Identity Federation on the same machine where you are installing Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Authorization Policy Manager, and Oracle Identity Navigator, then you will see a single IDM_Home directory, such as **Oracle_IDM1**, under your MW_HOME directory.

  For more information, see Overview and Structure of Oracle Identity Management 11g Installation.

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

  You must complete this additional configuration for Oracle Identity Manager components after configuring Oracle Identity Manager in a new or existing WebLogic administration domain. For more information, see the chapter Configuring Oracle Identity Manager.

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

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

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

Note that Oracle Identity Manager requires Oracle SOA Suite 11*g* (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 and Oracle SOA Suite are installed under the same Middleware Home directory and configured in the same WebLogic domain.

13.3 Domain Extension Scenarios

The following lists the scenarios in which you can extend an existing Oracle Identity Management domain to support new Oracle Identity Management products:

- Extending an Oracle Identity Management 11.1.1.3.0 Domain to Support OIM, OAM, OAAM, OAPM or OIN on the Local Machine
- Understanding Joint Configuration and Domain Extension Scenarios for OIM, OAM, OAAM, OAPM, and OIN on the Local Machine

13.3.1 Extending an Oracle Identity Management 11.1.1.3.0 Domain to Support OIM, OAM, OAAM, OAPM or OIN on the Local Machine

It is assumed that you have installed the latest versions of Oracle WebLogic Server and Oracle Identity Management before patching your Oracle Identity Management software to 11.1.1.3.0.

After the installation is complete, you must run the Patch Set Installer for Oracle Identity Management Suite to update your software to the latest version.

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

You should have installed and configured the Oracle Identity Management 11.1.1.3.0 products (Oracle Internet Directory, Oracle Virtual Directory, Oracle Directory Services Manager, Oracle Directory Integration Platform, or Oracle Identity Federation), before attempting to extend the 11.1.1.3.0 domain to support Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Authorization Policy Manager, or Oracle Identity Navigator.

This scenario involves the following tasks:

1. Installing the latest version of Oracle SOA 11*g* Suite (for Oracle Identity Manager only), as described in Installing the Latest Version of Oracle SOA Suite (Oracle Identity Manager Users Only).
2. Installing the Oracle Identity Management Suite under your existing Middleware Home, as described in Installing OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0).

3. Creating and loading the necessary schemas for the new components to be added, as described in Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU).
4. Launching the Oracle Fusion Middleware Configuration Wizard `<Oracle_IDM2>/common/bin/config.sh` script on UNIX (`<Oracle_IDM2>\common\bin\config.cmd` on Windows).
5. Selecting the **Extend an existing WebLogic domain** option on the Welcome screen.
6. Selecting the existing Oracle Identity Management 11.1.1.3.0 domain on the Select a WebLogic Domain Directory screen.
7. Selecting the required domain templates on the Select Extension Source screen to support Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Identity Navigator, or Oracle Authorization Policy Manager.
8. Modifying JDBC component schemas, configuration of Managed Servers, Deployments and Services, and so on.
9. Starting the Administration Server on the local machine, as described in Starting or Stopping the Oracle Stack.
10. Starting Managed Servers, as described in Starting or Stopping the Oracle Stack.

Note: When you extend an existing WebLogic domain to support Oracle Identity Manager, you should restart the Administration Server before launching the Oracle Identity Manager Configuration Wizard to configure Oracle Identity Manager Server.

13.3.2 Understanding Joint Configuration and Domain Extension Scenarios for OIM, OAM, OAAM, OAPM, and OIN on the Local Machine

It is assumed that you have installed the latest versions of Oracle WebLogic Server and the Oracle Identity Management Suite. For Oracle Identity Manager, you should have installed the latest version of Oracle SOA 11*g* Suite. You should have created and loaded the necessary schemas by using Oracle Fusion Middleware Repository Creation Utility (RCU).

You should have configured a new domain to support any of the various combinations of Oracle Access Manager (OAM), Oracle Adaptive Access Manager (OAAM), Oracle Identity Navigator (OIN), and Oracle Authorization Policy Manager (OAPM).

For example, you can configure Oracle Identity Manager in an existing Oracle Identity Management domain that contains Oracle Access Manager or Oracle Identity Navigator.

Several combinations are possible, based on your Oracle Identity Management environment and deployment.

This scenario involves the following tasks:

1. Creating and loading the necessary schemas for the new components to be added, as described in Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU).
2. Launching the Oracle Fusion Middleware Configuration Wizard `<Oracle_IDM2>/common/bin/config.sh` script on UNIX (`<Oracle_IDM2>\common\bin\config.cmd` on Windows).

3. Selecting the **Extend an existing WebLogic domain** option on the Welcome screen.
4. Selecting the existing Oracle Identity Management domain (the domain that contains any of the various combinations of Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Identity Navigator, and Oracle Authorization Policy Manager) on the Select a WebLogic Domain Directory screen.
5. Selecting the required domain templates on the Select Extension Source screen to support Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Identity Navigator, or Oracle Authorization Policy Manager. The choice of domain templates in this step depends on the component you are trying to configure in the same domain.
6. Modifying JDBC component schemas, configuration of Managed Servers, Deployments and Services, and so on.
7. Starting the Administration Server on the local machine, as described in Starting or Stopping the Oracle Stack.
8. Starting Managed Servers, as described in Starting or Stopping the Oracle Stack.

Note: When you extend an existing WebLogic domain to support Oracle Identity Manager, you should restart the Administration Server before launching the Oracle Identity Manager Configuration Wizard to configure Oracle Identity Manager Server.

13.4 Starting the Administration Server on the Local Machine

In some scenarios, you may want to install the Administration Server on one machine and component-specific Managed Servers on another machine. You must start the Administration Server on the machine where it is installed before you can create and run Managed Servers on the remote machine.

13.5 Creating Managed Servers on a Remote Machine

Before you can create and run Managed Servers on a remote machine, you must install Oracle WebLogic Server and Oracle Identity Management Suite on the remote machine. Then you must use the pack and unpack commands to create Managed Servers on the remote machine.

13.5.1 Installing Oracle WebLogic Server and Oracle Identity Management Suite on the Remote Machine

You must install Oracle WebLogic Server and Oracle Identity Management Suite on the remote machine.

- On the remote machine, install Oracle WebLogic Server and create a Middleware Home directory, as described in Installing Oracle WebLogic Server 10.3.3 and Creating the Oracle Middleware Home.

Note: The structure of Middleware Home and IDM Home directories on the remote machine should be identical to that of the local machine.

- On the remote machine, install Oracle Identity Management Suite, as described in Installing OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0).

After this installation, you can create and start Managed Servers on the remote machine, as described in the following topic.

13.5.2 Creating and Starting Managed Servers on a Remote Machine

To create and start a Managed Server on a remote machine, complete the following steps:

- On the local machine where the domain is configured and the Administration Server is created, use the `pack` command located in the `\common\bin` directory under your IDM_Home directory to create a Managed Server template that contains a subset of the files in a domain that are required to create a Managed Server domain directory hierarchy on a remote machine.

  The `-managed={true}` parameter of the `pack` command specifies whether the template is to be used to create Managed Servers on remote machines.
- Ensure that the Administration Server is up and running on the local machine.
- On the remote machine, use the `unpack` command located in the `\common\bin` directory under your IDM_Home directory to create the Managed Server domain directory on the remote machine.

Note: For Oracle Identity Manager users only:

If you want to start the SOA Server on a remote machine, then you must manually copy the composite files from the `<DOMAIN_HOME>/soa/autodeploy` directory on the local machine to the `<DOMAIN_HOME>/soa/autodeploy` directory on the remote machine after running the `unpack` command on the remote machine. If the `<DOMAIN_HOME>/soa/autodeploy` directory does not exist on the remote machine, you must create this directory before copying the composite files.

For more information, see the topic "Creating and Starting a Managed Server on a Remote Machine" in the guide *Oracle Fusion Middleware Creating Templates and Domains Using the Pack and Unpack Commands*. In addition, see the topic "Extending WebLogic Domains" in the guide *Oracle Fusion Middleware Creating Domains Using the Configuration Wizard*.

14

Oracle Identity Management Suite-Level Installation Scenarios

This chapter describes how to implement some of the most common and important Oracle Identity Management suite-level installation scenarios.

It discusses the following scenarios:

- General Prerequisites
- Important Notes Before You Begin
- Simultaneous configuration of OIN, OAPM, OAAM, OAM, and OIM
- OIM with LDAP Sync, and OAM
- OIM with LDAP Sync, OAM, and OAAM
- OIM with LDAP Sync in an Existing OAM Installation with LDAP Configured
- OIM with LDAP Sync in an Existing OAM and OAAM Installation with LDAP Configured
- OAM in an Existing OIM with LDAP Sync
- OAAM in an Existing OIM with LDAP Sync and OAAM

14.1 General Prerequisites

You must complete the following prerequisites before configuring Oracle Identity Management 11*g* Release 1 (11.1.1.3.0) products in any scenario:

1. Installing Oracle Database, as described in Installing Oracle Database.
2. Installing 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.
3. **For Oracle Identity Manager users only**: Installing Oracle SOA Suite 11*g* Release 1 (11.1.1.2.0) and patching it to 11.1.1.3.0, as described in Installing the Latest Version of Oracle SOA Suite (Oracle Identity Manager Users Only).
4. Creating and loading schemas using Oracle Fusion Middleware Repository Creation Utility (RCU), as described in Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU).
5. Installing the Oracle Identity Management 11*g* Release 1 (11.1.1.3.0) suite, as described in Installing OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0). The Oracle Identity Management suite contains Oracle Identity Manager (OIM), Oracle

Access Manager (OAM), Oracle Adaptive Access Manager (OAAM), Oracle Authorization Policy Manager (OAPM), and Oracle Identity Navigator (OIN).

14.2 Important Notes Before You Begin

Before you start installing and configuring Oracle Identity Management products in any of the scenarios discussed in this chapter, keep the following points in mind:

- It is assumed that you are installing Oracle Internet Directory, Oracle Virtual Directory, Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Identity Navigator, and Oracle SOA Suite on the same machine.

  Note: In this chapter, two IDM_Home directories are mentioned in descriptions and procedures. 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 document. You can specify any name for either of your IDM_Home directories. In addition, you can install the two Oracle Identity Management suites (one containing Oracle Internet Directory, Oracle Virtual Directory, Oracle Directory Services Manager, Oracle Directory Integration Platform, and Oracle Identity Federation; another containing Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Authorization Policy Manager, and Oracle Identity Navigator) 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.

  If you have not installed Oracle Internet Directory, Oracle Virtual Directory, Oracle Directory Services Manager, Oracle Directory Integration Platform, or Oracle Identity Federation on the same machine where you are installing Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Authorization Policy Manager, and Oracle Identity Navigator, then you will see a single IDM_Home directory, such as **Oracle_IDM1**, under your MW_HOME directory.

  For more information, see Overview and Structure of Oracle Identity Management 11g Installation.

- By performing the domain configuration procedures described in this chapter, you can create Managed Servers on a local machine (the machine on which the Administration Server is running). However, you can create and start Managed Servers for Oracle Identity Management components on a remote machine. For more information, see the "Creating and Starting a Managed Server on a Remote

Machine" topic in the guide *Oracle Fusion Middleware Creating Templates and Domains Using the Pack and Unpack Commands*.

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

  You must complete this additional configuration for Oracle Identity Manager components after configuring Oracle Identity Manager in a new or existing WebLogic administration domain. For more information, see the chapter Configuring Oracle Identity Manager.

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

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

  Note that Oracle Identity Manager requires Oracle SOA Suite 11*g* (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 and Oracle SOA Suite are configured in the same domain.

14.3 Simultaneous configuration of OIN, OAPM, OAAM, OAM, and OIM

This section discusses how to configure Oracle Identity Navigator (OIN), Oracle Authorization Policy Manager (OAPM), Oracle Access Manager (OAM), and Oracle Identity Manager (OIM).

It includes the following sections:

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

14.3.1 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, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Authorization Policy Manager, and Oracle Identity Navigator
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

14.3.2 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 11*g* Release 1 (11.1.1.3.0) suite containing Oracle Internet Directory (OID) and Oracle Virtual Directory (OVD) are installed, as described in Installing OID, OVD, ODSM, ODIP, and OIF (11.1.1.5.0).

  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 OID and OVD with ODSM in a New WebLogic Domain.
- Install Oracle Identity Management 11*g* Release 1 (11.1.1.3.0) 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 (OID), 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)

14.3.3 Scenario 1: OIM with LDAP Sync, OAM with LDAP, OAAM, OAPM, and OIN in a New WebLogic Domain

This section discusses the following topics:

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure

14.3.3.1 Appropriate Deployment Environment

Perform the configuration in this topic if you want to configure Oracle Identity Manager (OIM), Oracle Access Manager (OAM), Oracle Adaptive Access Manager (OAAM), Oracle Authorization Policy Manager (OAPM), and Oracle Identity Navigator (OIN) simultaneously in a new WebLogic administration domain. Then you can configure Oracle Access Manager to use Oracle Internet Directory (OID) as its LDAP Provider. You can also set up LDAP Sync for Oracle Identity Manager.

14.3.3.2 Components Deployed

Performing the configuration in this section deploys the following:

- WebLogic Administration Server
- A Managed Server each for Oracle Identity Manager, Oracle Access Manager, and Oracle Adaptive 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 Identity Navigator and Oracle Authorization Policy Manager applications on the Administration Server
- Administration Consoles for the Oracle Access Manager and Oracle Adaptive Access Manager on the Administration Server

14.3.3.3 Dependencies

The installation and configuration in this section depends on the following:

- Oracle WebLogic Server
- Installation of Oracle Identity Management Suite, as described in Installing OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0)
- Oracle Database
- Oracle SOA 11*g* Suite
- JDK (either Oracle WebLogic JRockit JDK or Sun JDK 1.6.0)
- Database schemas for Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Authorization Policy Manager. For more information about schemas specific to each product, see Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU).

14.3.3.4 Procedure

To configure Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Identity Navigator, and Oracle Authorization Policy Manager in a new WebLogic domain, complete the following steps:

1. Ensure that all the prerequisites, listed in Prerequisites, are satisfied. In addition, see Important Notes Before You Begin.
2. 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.
3. On the Welcome screen, select **Create a new WebLogic domain**, and click **Next**. The Select Domain Source screen appears.
4. On the Select Domain Source screen, ensure that the **Generate a domain configured automatically to support the following products:** option is selected.
5. Create a WebLogic administration domain, which supports the following products:
   - **Oracle Identity Manager - 11.1.1.3.0 [Oracle_IDM2]**
   - **Oracle Access Manager with Database Policy Store - 11.1.1.3.0 [Oracle_IDM2]**
   - **Oracle Adaptive Access Manager Admin Server - 11.1.1.3.0 [Oracle_IDM2]**
   - **Oracle Identity Navigator - 11.1.1.3.0 [Oracle_IDM2]**
   - Optional: **Oracle Adaptive Access Manager Server - 11.1.1.3.0 [Oracle_IDM2]**
   - **Oracle Authorization Policy Manager - 11.1.1.3.0 [Oracle_IDM2]**

   Note: When you select any the Oracle Identity Management products, the **Oracle JRF 11.1.1.0 [oracle_common]** option is also selected automatically.

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

   Click **Next**. The Specify Domain Name and Location screen appears
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 160_17_R28.0.0-679` 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 displays a list of the following component schemas:
   - SOA Infrastructure
   - User Messaging Service

- OAAM Server Schema
- OIM MDS Schema
- OWSM MDS Schema
- OAAM Admin Server
- OAAM Admin MDS Schema
- APM MDS Schema
- APM Schema
- OIM Schema
- SOA MDS Schema
- OAM Infrastructure

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

      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.
    - Optional: Configure RDBMS Security Store, as required.
11. On the Configuration Summary screen, you can view the summary of your configuration for deployments, application, and service. Review the domain configuration, and click **Create** to start creating the domain.

    A WebLogic domain to support Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Authorization Policy 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.

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

13. 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=oracle,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*.

14. Set up LDAP Synchronization for Oracle Identity Manager, as described in Setting Up LDAP Synchronization.
15. Verify LDAP Synchronization, as described in Verifying the LDAP Synchronization.
16. Start the Oracle Identity Manager Configuration Wizard, as described in Starting the Oracle Identity Manager 11g Configuration Wizard.
17. 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.
18. 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.

14.3.4 Scenario 2: OIM with LDAP Sync, OAM with LDAP, OAAM, OAPM, and OIN in an Existing Domain Containing OID and OVD

This section discusses the following topics:

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure

14.3.4.1 Appropriate Deployment Environment

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

- You want to add Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Authorization Policy Manager, and Oracle Identity Navigator to an existing Oracle Identity Management domain that contains Oracle Internet Directory and Oracle Virtual Directory.
- You want to configure all Oracle Identity Management products, including 11.1.1.3.0, in the same WebLogic administration domain.
- You want a single WebLogic Administration Server to manage all of the Oracle Identity Management 11*g* products.

14.3.4.2 Components Deployed

Performing the configuration in this section deploys the following components:

- A Managed Server each for Oracle Identity Manager, Oracle Access Manager, and Oracle Adaptive Access Manager
- Oracle Identity Manager, Oracle Access Manager, and Oracle Adaptive Access Manager applications on Managed Servers
- Administration Consoles for Oracle Access Manager and Oracle Adaptive Access Manager on the existing Administration Server

- Oracle Identity Navigator application and Oracle Authorization Policy Manager on the existing Administration Server
- Oracle Identity Administration Console, Oracle Identity Manager Self Service Console, and Oracle Identity Manager Advanced Administration Console on the Oracle Identity Manager Managed Server

14.3.4.3 Dependencies

The configuration in this section depends on the following:

- Oracle WebLogic Server
- Installation of Oracle Identity Management Suite, as described in Installing OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0)
- Oracle Database
- Oracle SOA 11*g* Suite
- JDK (either Oracle WebLogic JRockit JDK or Sun JDK 1.6.0)
- Database schemas for Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Authorization Policy Manager. For more information about schemas specific to each product, see Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU).

14.3.4.4 Procedure

To extend an existing Oracle Identity Management 11.1.1.3.0 domain (the domain with Oracle Internet Directory and Oracle Virtual Directory) to support Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Authorization Policy Manager, and Oracle Identity Navigator, complete the following steps:

1. Ensure that all the prerequisites, listed in Prerequisites, are satisfied. In addition, see Important Notes Before You Begin.
2. 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.
3. On the Select Domain screen, select the **Create New Domain** option. Set the Administrator user name and password, as required.
4. Ensure that you select **Oracle Internet Directory** and **Oracle Virtual Directory** on the Configure Components screen.
5. 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.
6. Ensure that your Oracle database version is supported and you have installed the necessary patches. For more information, see Installing Oracle Database.
7. 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).

8. 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.
9. 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.
10. 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.
11. On the Welcome screen, select the **Extend an existing WebLogic domain** option. Click **Next**. The Select a WebLogic Domain Directory screen is displayed.
12. On the Select a WebLogic Domain Directory screen, select the directory that contains the domain in which you configured Oracle Internet Directory and Oracle Virtual Directory. Click **Next**.
13. On the Select Domain Source screen, ensure that the **Extend my domain to automatically to support the following added products:** is selected.
14. Select the following options:
    - **Oracle Identity Manager - 11.1.1.3.0 [Oracle_IDM2]**
    - **Oracle Access Manager with Database Policy Store - 11.1.1.3.0 [Oracle_IDM2]**
    - **Oracle Adaptive Access Manager Admin Server - 11.1.1.3.0 [Oracle_IDM2]**
    - **Oracle Authorization Policy Manager - 11.1.1.3.0 [Oracle_IDM2]**
    - **Oracle Identity Navigator - 11.1.1.3.0 [Oracle_IDM2]**

    Note: When you select the **Oracle Identity Manager - 11.1.1.3.0 [Oracle_IDM2]** option, the **Oracle SOA Suite - 11.1.1.0 [Oracle_SOA1]** option, and the **Oracle WSM Policy Manager - 11.1.1.0 [oracle_common]** option are also selected.
15. Click **Next**. The Configure JDBC Component Schema appears.

    The screen displays a list of the following component schemas:
    - SOA Infrastructure
    - User Messaging Service
    - OAAM Admin Schema
    - OAAM Admin MDS Schema
    - APM Schema
    - APM MDS Schema
    - OIM MDS Schema
    - OWSM MDS Schema
    - SOA MDS Schema
    - OAM Infrastructure

- OIM Schema

16. 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.
17. 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.

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

    Your existing Oracle Identity Management domain with Oracle Internet Directory and Oracle Virtual Directory is configured to support Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Authorization Policy Manager, and Oracle Identity Navigator.
19. Start the WebLogic Administration Server and Managed Servers (Oracle Identity Manager and Oracle Access Manager), as described in Starting the Stack.
20. 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*.

21. Set up LDAP Synchronization for Oracle Identity Manager, as described in Setting Up LDAP Synchronization.
22. Verify LDAP Synchronization, as described in Verifying the LDAP Synchronization.
23. Restart the Administration Server, as described in Restarting Servers.
24. Start the Oracle Identity Manager Configuration Wizard, as described in Starting the Oracle Identity Manager 11g Configuration Wizard.
25. 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.
26. 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.

14.4 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
- Scenario 3: OIM with LDAP Sync, and OAM, in a Domain Containing OAAM, OAPM, and OIN

14.4.1 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

14.4.2 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 11*g* Release 1 (11.1.1.3.0) suite containing Oracle Internet Directory (OID) and Oracle Virtual Directory (OVD) are installed, as described in Installing OID, OVD, ODSM, ODIP, and OIF (11.1.1.5.0).

  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 OID and OVD with ODSM in a New WebLogic Domain.
- Install Oracle Identity Management 11*g* Release 1 (11.1.1.3.0) 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)

14.4.3 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

14.4.3.1 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. You can set up this integration, as described in Integration Between OIM and OAM.

14.4.3.2 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

14.4.3.3 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).

14.4.3.4 Procedure

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

1. Ensure that all the prerequisites, listed in Prerequisites, are satisfied. In addition, see Important Notes Before You Begin.
2. 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.
3. On the Welcome screen, select the **Create a new WebLogic domain** option. Click **Next**. The Select Domain Source screen is displayed.
4. 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]**
5. After selecting the domain configuration options, click **Next**. The Specify Domain Name and Location screen is displayed.
6. 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.
7. 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.
8. Choose `JRockit SDK 160_17_R28.0.0-679` 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.
9. 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.

10. 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 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.

      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.
11. 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.
12. Start the WebLogic Administration Server and Managed Servers (Oracle Identity Manager and Oracle Access Manager), as described in Starting the Stack.
13. 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=oracle,dc=com"
,ldapUrl="ldap://<oid host>:<oid port>" ,isPrimary="true"
,userIDProvider="OracleUserRoleAPI" ,
groupSearchBase="cn=Groups,dc=us,dc=oracle,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 use one of the following options:

- 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.
- The admin can create it using Oracle Directory Services Manager (ODSM)

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*.

14. Set up LDAP Synchronization for Oracle Identity Manager, as described in Setting Up LDAP Synchronization.
15. Verify LDAP Synchronization, as described in Verifying the LDAP Synchronization.
16. Start the Oracle Identity Manager Configuration Wizard, as described in Starting the Oracle Identity Manager 11g Configuration Wizard.
17. 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.
18. 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.

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

14.4.4 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

14.4.4.1 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), as described in Integration Between OIM and OAM.

14.4.4.2 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

14.4.4.3 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).

14.4.4.4 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. Ensure that all the prerequisites, listed in Prerequisites, are satisfied. In addition, see Important Notes Before You Begin.
2. 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.
3. On the Select Domain screen, select the **Create New Domain** option. Set the Administrator user name and password, as required.
4. Ensure that you select **Oracle Internet Directory** and **Oracle Virtual Directory** on the Configure Components screen.
5. 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.
6. Ensure that your Oracle database version is supported and you have installed the necessary patches. For more information, see Installing Oracle Database.
7. 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).
8. 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.
9. 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.
10. 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.
11. On the Welcome screen, select the **Extend an existing WebLogic domain** option. Click **Next**. The Select a WebLogic Domain Directory screen is displayed.
12. 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.
13. 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]**

14. After selecting the domain configuration options, click **Next**. The Configure JDBC Component Schema screen is displayed.
15. 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.
16. 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 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.

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

19. 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=oracle,dc=com"
    ,ldapUrl="ldap://<oid host>:<oid port>" ,isPrimary="true"
    ,userIDProvider="OracleUserRoleAPI" ,
    groupSearchBase="cn=Groups,dc=us,dc=oracle,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 use one of the following options:

    - 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.
    - The admin can create it using Oracle Directory Services Manager (ODSM)

    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*.

20. Set up LDAP Synchronization for Oracle Identity Manager, as described in Setting Up LDAP Synchronization.

21. Verify LDAP Synchronization, as described in Verifying the LDAP Synchronization.
22. Restart the Administration Server, as described in Restarting Servers.
23. Start the Oracle Identity Manager Configuration Wizard, as described in Starting the Oracle Identity Manager 11g Configuration Wizard.
24. 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.
25. 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.

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

14.4.5 Scenario 3: OIM with LDAP Sync, and OAM, in a Domain Containing OAAM, OAPM, and OIN

This section discusses the following topics:

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure

14.4.5.1 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 other Oracle Identity Management products, such as Oracle Adaptive Access Manager (OAAM), Oracle Authorization Policy Manager (OAPM), and Oracle Identity Navigator (OIN) are installed and configured.

At a later time, you may set up integration between Oracle Identity Manager and Oracle Access Manager, as described in Integration Between OIM and OAM.

You can use Oracle Identity Navigator to discover and launch Consoles for the Oracle Identity Management products from within the Oracle Identity Navigator user interface.

14.4.5.2 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

14.4.5.3 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).

14.4.5.4 Procedure

Perform the following steps to configure Oracle Identity Manager with LDAP Synchronization, and Oracle Access Manager in an existing Oracle Identity Management domain that contains Oracle Adaptive Access Manager, Oracle Authorization Policy Manager, and Oracle Identity Navigator:

1. Ensure that all the prerequisites, listed in Prerequisites, are satisfied. In addition, see Important Notes Before You Begin.
2. 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.
3. On the Welcome screen, select the **Create a new WebLogic domain** option. Click **Next**. The Select Domain Source screen is displayed.
4. On the Select Domain Source screen, select the following domain configuration options:
   - **Oracle Adaptive Access Manager Admin Server - 11.1.1.3.0 [Oracle_IDM2]**

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

   - **Oracle Authorization Policy Manager - 11.1.1.3.0 [Oracle_IDM2]**
5. After selecting the domain configuration options, click **Next**. The Specify Domain Name and Location screen is displayed.
6. 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.

7. 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.
8. Choose `JRockit SDK 160_17_R28.0.0-679` 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.
9. On the Configure JDBC Component Schema screen, select a component schema, such as the OAAM Admin Schema, the APM Schema, the APM MDS Schema, or the OAAM Admin MDS Schema, that you want to modify.

   You can set values for Schema Owner, Schema Password, Database and Service, Host Name, and Port. Click **Next**. The Test JDBC Component Schema screen appears. After the test succeeds, the Select Optional Configuration screen appears.
10. On the Select Optional Configuration screen, you can configure **Administration Server, Managed Servers, Clusters, and Machines**, **Deployments and Services**, and **RDBMS Security 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 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.

      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.
11. On the Configuration Summary screen, review the domain configuration, and click **Create** to start creating the domain. After the domain configuration is complete, click **Done** to dismiss the wizard.

    A new WebLogic domain to support Oracle Authorization Policy Manager and Oracle Adaptive Access Manager, and Oracle Identity Navigator is created in the `<MW_HOME>\user_projects\domains` directory (on Windows), by default. On UNIX, the domain is created in the `<MW_HOME>/user_projects/domains` directory, by default.
12. 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.

13. On the Welcome screen, select the **Extend an existing WebLogic domain** option. Click **Next**. The Select a WebLogic Domain Directory screen is displayed.
14. On the Select a WebLogic Domain Directory screen, select the Oracle Identity Management domain in which you configured Oracle Authorization Policy Manager and Oracle Adaptive Access Manager, and Oracle Identity Navigator. Click **Next**. The Select Extension Source screen is displayed.
15. 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]**
16. After selecting the domain configuration options, click **Next**. The Configure JDBC Component Schema screen is displayed.
17. On the Configure JDBC Component Schema screen, select a component schema, such as the OAM Infrastructure Schema, the SOA Infrastructure Schema, the OAAM Admin Schema, the APM Schema, the APM MDS Schema, the OAAM Admin MDS 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.
18. 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 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.

      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.

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

    Your existing Oracle Identity Management domain with Oracle Authorization Policy Manager and Oracle Adaptive Access Manager, and Oracle Identity Navigator is extended to support Oracle Identity Manager and Oracle Access Manager.

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

21. 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=oracle,dc=com"
       ,ldapUrl="ldap://<oid host>:<oid port>" ,isPrimary="true"
       ,userIDProvider="OracleUserRoleAPI" ,
       groupSearchBase="cn=Groups,dc=us,dc=oracle,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*.

22. Set up LDAP Synchronization for Oracle Identity Manager, as described in Setting Up LDAP Synchronization.
23. Verify LDAP Synchronization, as described in Verifying the LDAP Synchronization.
24. Restart the Administration Server, as described in Restarting Servers.
25. Start the Oracle Identity Manager Configuration Wizard, as described in Starting the Oracle Identity Manager 11g Configuration Wizard.
26. 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.
27. 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.

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

14.5 OIM with LDAP Sync, OAM, and OAAM

This topic describes how to configure Oracle Identity Manager (OIM) with LDAP Synchronization, Oracle Access Manager (OAM), and Oracle Adaptive Access Manager (OAAM) in a new or existing WebLogic domain.

It includes the following sections:

- Overview
- Prerequisites
- Scenario 1: OIM with LDAP Sync, and OAM in a New WebLogic Domain
- Scenario 2: Configuration in a Domain Containing OID and OVD
- Scenario 3: Configuration in a Domain Containing OAPM and OIN

14.5.1 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, Oracle Access Manager, and Oracle Adaptive 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

14.5.2 Prerequisites

The following lists the prerequisites for installing and configuring Oracle Identity Manager with LDAP Synchronization, Oracle Access Manager, and Oracle Adaptive 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 11*g* Release 1 (11.1.1.3.0) suite containing Oracle Internet Directory (OID) and Oracle Virtual Directory (OVD) are installed, as described in Installing OID, OVD, ODSM, ODIP, and OIF (11.1.1.5.0).

  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 OID and OVD with ODSM in a New WebLogic Domain.
- Install Oracle Identity Management 11*g* Release 1 (11.1.1.3.0) 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)

14.5.3 Scenario 1: Configuration in a New WebLogic Domain

This section discusses the following topics:

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure

14.5.3.1 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, as described in Integration Between OIM and OAM.

You may add other Oracle Identity Management products, such as Oracle Authorization Policy Manager and Oracle Identity Navigator at a later time in the same domain.

14.5.3.2 Components Deployed

Performing the configuration in this section deploys the following:

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

14.5.3.3 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, Oracle Adaptive Access Manager, and Oracle Access Manager. For more information, see Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU).

14.5.3.4 Procedure

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

1. Ensure that all the prerequisites, listed in Prerequisites, are satisfied. In addition, see Important Notes Before You Begin.
2. Run the `<Oracle_IDM2>/common/bin/config.sh` script on UNIX (`<IDM_Home>\common\bin\config.cmd` on Windows). The Oracle Fusion Middleware Configuration Wizard appears.

3. On the Welcome screen, select the **Create a new WebLogic domain** option. Click **Next**. The Select Domain Source screen is displayed.
4. 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]**, **Oracle JRF - 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]**
   - **Oracle Adaptive Access Manager Admin Server - 11.1.1.3.0 [Oracle_IDM2]**

     When you select the **Oracle Adaptive Access Manager Admin Server - 11.1.1.3.0 [Oracle_IDM2}** option, the **Oracle Identity Navigator - 11.1.1.3.0 [Oracle_IDM2]** option is also selected, by default.
5. After selecting the domain configuration options, click **Next**. The Specify Domain Name and Location screen is displayed.
6. 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.
7. 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.
8. Choose `JRockit SDK 160_17_R28.0.0-679` 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.
9. On the Configure JDBC Component Schema screen, select a component schema, such as the OAAM Admin Schema, the OAAM Admin MDS 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.
10. On the Select Optional Configuration screen, you can configure **Administration Server, JMS Distributed Destination, 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: Select 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 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.

  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.

11. 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, Oracle Adaptive Access Manager, and Oracle Access Manager is created in the `<MW_HOME>\user_projects\domains` directory (on Windows), by default. On UNIX, the domain is created in the `<MW_HOME>/user_projects/domains` directory, by default.

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

13. 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=oracle,dc=com"
,ldapUrl="ldap://<oid host>:<oid port>" ,isPrimary="true"
,userIDProvider="OracleUserRoleAPI" ,
groupSearchBase="cn=Groups,dc=us,dc=oracle,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*.

14. Set up LDAP Synchronization for Oracle Identity Manager, as described in Setting Up LDAP Synchronization.
15. Verify LDAP Synchronization, as described in Verifying the LDAP Synchronization.
16. Start the Oracle Identity Manager Configuration Wizard, as described in Starting the Oracle Identity Manager 11g Configuration Wizard.
17. 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.
18. 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.

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

14.5.4 Scenario 2: Configuration in a Domain Containing OID and OVD

This section discusses the following topics:

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure

14.5.4.1 Appropriate Deployment Environment

Perform the configuration in this topic if you want to install Oracle Access Manager (OAM), Oracle Adaptive Access Manager (OAAM), and 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, as described in Integration Between OIM and OAM.

14.5.4.2 Components Deployed

Performing the configuration in this section deploys the following:

- Managed Servers for Oracle Identity Manager, Oracle Adaptive Access 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 and Oracle Adaptive Access Manager Console on the existing Administration Server

14.5.4.3 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, Oracle Adaptive Access Manager, and Oracle Access Manager. For more information, see Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU).

14.5.4.4 Procedure

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

1. Ensure that all the prerequisites, listed in Prerequisites, are satisfied. In addition, see Important Notes Before You Begin.
2. 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.

3. On the Select Domain screen, select the **Create New Domain** option. Set the Administrator user name and password, as required.
4. Ensure that you select **Oracle Internet Directory** and **Oracle Virtual Directory** on the Configure Components screen.
5. 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.
6. Ensure that your Oracle database version is supported and you have installed the necessary patches. For more information, see Installing Oracle Database.
7. 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).
8. 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.
9. 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.
10. 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.
11. On the Welcome screen, select the **Extend an existing WebLogic domain** option. Click **Next**. The Select a WebLogic Domain Directory screen is displayed.
12. 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.
13. 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]**
    - **Oracle Adaptive Access Manager Admin Server - 11.1.1.3.0 [Oracle_IDM2]**

      When you select the **Oracle Adaptive Access Manager Admin Server - 11.1.1.3.0 [Oracle_IDM2}** option, the **Oracle Identity Navigator - 11.1.1.3.0 [Oracle_IDM2]** option is also selected, by default.

14. After selecting the domain configuration options, click **Next**. The Configure JDBC Component Schema screen is displayed.
15. On the Configure JDBC Component Schema screen, select a component schema, such as the OAM Infrastructure Schema, the OAAM Admin Schema, the OAAM Admin MDS 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.
16. 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 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.

      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.
17. 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, Oracle Adaptive Access Manager, and Oracle Access Manager.
18. Start the WebLogic Administration Server and Managed Servers (Oracle Identity Manager and Oracle Access Manager), as described in Starting the Stack.
19. 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=oracle,dc=com"
,ldapUrl="ldap://<oid host>:<oid port>" ,isPrimary="true"
,userIDProvider="OracleUserRoleAPI" ,
groupSearchBase="cn=Groups,dc=us,dc=oracle,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*.

20. Set up LDAP Synchronization for Oracle Identity Manager, as described in Setting Up LDAP Synchronization.
21. Verify LDAP Synchronization, as described in Verifying the LDAP Synchronization.
22. Start the Oracle Identity Manager Configuration Wizard, as described in Starting the Oracle Identity Manager 11g Configuration Wizard.
23. 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.
24. 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.

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

14.5.5 Scenario 3: Configuration in a Domain Containing OAPM and OIN

This section discusses the following topics:

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure

14.5.5.1 Appropriate Deployment Environment

Perform the configuration in this topic if you want to install Oracle Access Manager (OAM), Oracle Adaptive Access Manager (OAAM), and Oracle Identity Manager (OIM) with LDAP Synchronization, in an environment where other Oracle Identity Management products, such as Oracle Authorization Policy Manager (OAPM) and Oracle Identity Navigator (OIN) are installed and configured.

At a later time, you may set up integration between Oracle Identity Manager and Oracle Access Manager, as described in Integration Between OIM and OAM.

You can use Oracle Identity Navigator to discover and launch Consoles for the Oracle Identity Management products from within the Oracle Identity Navigator user interface.

14.5.5.2 Components Deployed

Performing the configuration in this section deploys the following:

- Managed Servers for Oracle Identity Manager, Oracle Adaptive Access 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 and Oracle Adaptive Access Manager Console on the existing Administration Server

14.5.5.3 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, Oracle Adaptive Access Manager, and Oracle Access Manager. For more information, see Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU).

14.5.5.4 Procedure

Perform the following steps to configure Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager with LDAP Synchronization, in an existing Oracle Identity Management domain that contains Oracle Authorization Policy Manager and Oracle Identity Navigator:

1. Ensure that all the prerequisites, listed in Prerequisites, are satisfied. In addition, see Important Notes Before You Begin.
2. 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.
3. On the Welcome screen, select the **Create a new WebLogic domain** option. Click **Next**. The Select Domain Source screen is displayed.
4. On the Select Domain Source screen, select the following domain configuration options:
   - **Oracle Authorization Policy Manager - 11.1.1.3.0 [Oracle_IDM2]**

     Note: When you select the **Oracle Authorization Policy Manager - 11.1.1.3.0 [Oracle_IDM2]** option, the following option is also selected, by default: **Oracle JRF - 11.1.1.0 [oracle_common]**.

   - **Oracle Identity Navigator - 11.1.1.3.0 [Oracle_IDM2]**
5. After selecting the domain configuration options, click **Next**. The Specify Domain Name and Location screen is displayed.
6. 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.
7. 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.
8. Choose `JRockit SDK 160_17_R28.0.0-679` 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.
9. On the Configure JDBC Component Schema screen, select a component schema, such as the APM Schema, or the APM 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.

10. On the Select Optional Configuration screen, you can configure **Administration Server, Managed Servers, Clusters, and Machines**, **Deployments and Services**, and **RDBMS Security 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 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.

      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.
11. On the Configuration Summary screen, review the domain configuration, and click **Create** to start creating the domain. After the domain configuration is complete, click **Done** to dismiss the wizard.

    A new WebLogic domain to support Oracle Authorization Policy Manager and Oracle Identity Navigator is created in the `<MW_HOME>\user_projects\domains` directory (on Windows), by default. On UNIX, the domain is created in the `<MW_HOME>/user_projects/domains` directory, by default.
12. 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.
13. On the Welcome screen, select the **Extend an existing WebLogic domain** option. Click **Next**. The Select a WebLogic Domain Directory screen is displayed.
14. On the Select a WebLogic Domain Directory screen, select the Oracle Identity Management domain in which you configured Oracle Authorization Policy Manager and Oracle Identity Navigator. Click **Next**. The Select Extension Source screen is displayed.
15. 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]**
- **Oracle Adaptive Access Manager Admin Server - 11.1.1.3.0 [Oracle_IDM2]**

  When you select the **Oracle Adaptive Access Manager Admin Server - 11.1.1.3.0 [Oracle_IDM2}** option, the **Oracle Identity Navigator - 11.1.1.3.0 [Oracle_IDM2]** option is also selected, by default.

16. After selecting the domain configuration options, click **Next**. The Specify Domain Name and Location screen is displayed.
17. On the Specify Domain Name and Location screen, select a location to store the applications in the domain. Click **Next**. The Configure JDBC Component Schema screen is displayed.
18. On the Configure JDBC Component Schema screen, select a component schema, such as the OAM Infrastructure Schema, the SOA Infrastructure Schema, the OAAM Admin Schema, the APM Schema, the APM MDS Schema, the OAAM Admin MDS 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.
19. 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.

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

    Your existing Oracle Identity Management domain with Oracle Authorization Policy Manager and Oracle Identity Navigator is extended to support Oracle Identity Manager, Oracle Adaptive Access Manager, and Oracle Access Manager.

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

22. 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=oracle,dc=com"
    ,ldapUrl="ldap://<oid host>:<oid port>" ,isPrimary="true"
    ,userIDProvider="OracleUserRoleAPI" ,
    groupSearchBase="cn=Groups,dc=us,dc=oracle,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*.

23. Set up LDAP Synchronization for Oracle Identity Manager, as described in Setting Up LDAP Synchronization.

24. Verify LDAP Synchronization, as described in Verifying the LDAP Synchronization.

25. Restart the Administration Server, as described in Restarting Servers.
26. Start the Oracle Identity Manager Configuration Wizard, as described in Starting the Oracle Identity Manager 11g Configuration Wizard.
27. 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.
28. Follow the wizard and the steps described in Configuring OIM Server to complete the Oracle Identity ManagerServer 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.

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

14.6 OIM with LDAP Sync in an Existing OAM Installation with LDAP Configured

This section describes how to configure Oracle Identity Manager (OIM) with LDAP Sync to an existing Oracle Access Manager installation, which has Oracle Internet Directory (OID) configured as the LDAP provider.

It contains the following sections:

- Overview
- Prerequisites
- Scenario 1: Configuration in a New WebLogic Domain
- Scenario 2: Configuration in a Domain Containing OID and OVD
- Scenario 3: Configuration in a Domain Containing OAAM, OAPM, and OIN

14.6.1 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 Access Manager
3. Configure Oracle Access Manager to use Oracle Internet Directory as the LDAP provider
4. Configure Oracle Identity Manager
5. Set up LDAP sync for Oracle Identity Manager
6. Configure Oracle Identity Manager Server, Design Console (Windows only), and Remote Manager

14.6.2 Prerequisites

The following lists the prerequisites for installing and configuring Oracle Identity Manager with LDAP Synchronization to an existing Oracle Access Manager installation, which has LDAP configured:

- 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 11*g* Release 1 (11.1.1.3.0) suite containing Oracle Internet Directory (OID) and Oracle Virtual Directory (OVD) are installed, as described in Installing OID, OVD, ODSM, ODIP, and OIF (11.1.1.5.0).

  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 OID and OVD with ODSM in a New WebLogic Domain.
- Install Oracle Identity Management 11*g* Release 1 (11.1.1.3.0) 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)

14.6.3 Scenario 1: Configuration in a New WebLogic Domain

This section discusses the following topics:

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure

14.6.3.1 Appropriate Deployment Environment

Perform configuration in this section for Oracle Identity Management environments that have the following conditions:

- Oracle Internet Directory, Oracle Virtual Directory, Oracle Access Manager, and Oracle Identity Manager are installed on the same machine.
- Oracle Access Manager is configured in a new WebLogic domain, which is extended to support Oracle Identity Manager at a later time.
- Oracle Access Manager is configured to use Oracle Internet Directory as the LDAP provider before configuring LDAP Sync for Oracle Identity Manager.

14.6.3.2 Components Deployed

Performing this configuration deploys the following:

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

14.6.3.3 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, Oracle Adaptive Access Manager, and Oracle Access Manager. For more information, see Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU).

14.6.3.4 Procedure

Perform the following steps to configure Oracle Identity Manager with LDAP Synchronization, to an existing Oracle Access Manager installation, which has LDAP configured:

1. Ensure that all the prerequisites, listed in Prerequisites, are satisfied. In addition, see Important Notes Before You Begin.
2. Run the `<Oracle_IDM2>/common/bin/config.sh` script (`<Oracle_IDM2>\common\bin\config.cmd` on Windows). The Oracle Fusion Middleware Configuration Wizard appears.
3. On the Welcome screen, select the **Create a new WebLogic domain** option. Click **Next**. The Select Domain Source screen is displayed.
4. On the Select Domain Source screen, ensure that the **Generate a domain configured automatically to support the following products:** option is selected.

Select **Oracle Access Manager with Database Policy Store - 11.1.1.3.0 [Oracle_IDM2]**, and click **Next**. The Select Domain Name and Location screen appears.

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

---

5. After selecting the domain configuration options, click **Next**. The Specify Domain Name and Location screen is displayed.
6. 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.
7. 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.
8. Choose `JRockit SDK 160_17_R28.0.0-679` 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.
9. On the Configure JDBC Component Schema screen, select a component schema, such as the OAM Infrastructure Schema, that you want to modify.

   You can set values for Schema Owner, Schema Password, Database and Service, Host Name, and Port. Click **Next**. The Test JDBC Component Schema screen appears. After the test succeeds, the Select Optional Configuration screen appears.
10. On the Select Optional Configuration screen, you can configure **Administration Server, Managed Servers, Clusters, and Machines**, and **RDBMS Security Store**. Select the relevant check boxes and click **Next**.
    - Optional: Configure Administration Server, as required.
    - Optional: Select 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 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.

      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: Configure RDBMS Security Store, as required.

11. 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), by default. On UNIX, the domain is created in the `<MW_HOME>/user_projects/domains` directory, by default.

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

13. 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=oracle,dc=com"
       ,ldapUrl="ldap://<oid host>:<oid port>" ,isPrimary="true"
       ,userIDProvider="OracleUserRoleAPI" ,
       groupSearchBase="cn=Groups,dc=us,dc=oracle,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*.

14. 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.
15. On the Welcome screen, select the **Extend an existing WebLogic domain** option. Click **Next**. The Select a WebLogic Domain Directory screen is displayed.
16. On the Select a WebLogic Domain Directory screen, select the Oracle Identity Management domain in which you configured Oracle Access Manager. Click **Next**. The Select Extension Source screen is displayed.
17. 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]**, **Oracle Enterprise Manager - 11.1.1.0 [oracle_common]**, and **Oracle WSM Policy Manager - 11.1.1.0 [oracle_common]**.
18. After selecting the domain configuration options, click **Next**. The Specify Domain Name and Location screen is displayed.
19. On the Specify Domain Name and Location screen, select a location to store the applications in the domain. Click **Next**. The Configure JDBC Component Schema screen is displayed.
20. 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.
21. 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.

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.

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

    Your existing Oracle Identity Management domain with Oracle Access Manager is extended to support Oracle Identity Manager.

23. Set up LDAP Synchronization for Oracle Identity Manager, as described in Setting Up LDAP Synchronization.

24. Verify LDAP Synchronization, as described in Verifying the LDAP Synchronization.

25. Start the Oracle Identity Manager Configuration Wizard, as described in Starting the Oracle Identity Manager 11g Configuration Wizard.

26. 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.

27. 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.

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

14.6.4 Scenario 2: Configuration in a Domain Containing OID and OVD

This section discusses the following topics:

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure

14.6.4.1 Appropriate Deployment Environment

Perform configuration in this section for Oracle Identity Management environments that have the following conditions:

- Oracle Internet Directory, Oracle Virtual Directory, Oracle Access Manager, and Oracle Identity Manager are installed on the same machine.
- Oracle Access Manager is configured in the existing Oracle Identity Management domain containing Oracle Internet Directory and Oracle Virtual Directory. This domain is extended to support Oracle Identity Manager at a later time.
- Oracle Access Manager is configured to use Oracle Internet Directory as the LDAP provider before configuring LDAP Sync for Oracle Identity Manager.

14.6.4.2 Components Deployed

Performing this configuration deploys the following:

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

14.6.4.3 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, Oracle Adaptive Access Manager, and Oracle Access Manager. For more information, see Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU).

14.6.4.4 Procedure

Perform the following steps to configure Oracle Identity Manager with LDAP Synchronization, to an existing Oracle Access Manager installation, which has LDAP configured:

1. Ensure that all the prerequisites, listed in Prerequisites, are satisfied. In addition, see Important Notes Before You Begin.
2. 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.
3. On the Select Domain screen, select the **Create New Domain** option. Set the Administrator user name and password, as required.
4. Ensure that you select **Oracle Internet Directory** and **Oracle Virtual Directory** on the Configure Components screen.
5. 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.

6. Ensure that your Oracle database version is supported and you have installed the necessary patches. For more information, see Installing Oracle Database.
7. 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).
8. 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.
9. 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.
10. 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.
11. On the Welcome screen, select the **Extend an existing WebLogic domain** option. Click **Next**. The Select a WebLogic Domain Directory screen is displayed.
12. 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.
13. On the Select Extension Source screen, select the following domain configuration options:

    Oracle Access Manager with Database Policy Store - 11.1.1.3.0 [Oracle_IDM2]
14. After selecting the domain configuration options, click **Next**. The Configure JDBC Component Schema screen is displayed.
15. On the Configure JDBC Component Schema screen, select a component schema, such as the OAM Infrastructure Schema, that you want to modify.

    You can set values for Schema Owner, Schema Password, Database and Service, Host Name, and Port. Click **Next**. The Test JDBC Component Schema screen appears. After the test succeeds, the Select Optional Configuration screen appears.
16. On the Select Optional Configuration screen, you can configure **Managed Servers, Clusters, and Machines**, **Deployments and Services**. 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.

  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.

17. 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 Access Manager.

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

19. 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=oracle,dc=com"
       ,ldapUrl="ldap://<oid host>:<oid port>" ,isPrimary="true"
       ,userIDProvider="OracleUserRoleAPI" ,
       groupSearchBase="cn=Groups,dc=us,dc=oracle,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*.

20. 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.
21. On the Welcome screen, select the **Extend an existing WebLogic domain** option. Click **Next**. The Select a WebLogic Domain Directory screen is displayed.
22. On the Select a WebLogic Domain Directory screen, select the Oracle Identity Management domain in which you configured Oracle Access Manager, Oracle Internet Directory and Oracle Virtual Directory. Click **Next**. The Select Extension Source screen is displayed.
23. 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]**, **Oracle Enterprise Manager - 11.1.1.0 [oracle_common]**, and **Oracle WSM Policy Manager - 11.1.1.0 [oracle_common]**.

24. After selecting the domain configuration options, click **Next**. The Specify Domain Name and Location screen is displayed.
25. On the Specify Domain Name and Location screen, select a location to store the applications in the domain. Click **Next**. The Configure JDBC Component Schema screen is displayed.
26. 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.

27. 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.

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

    Your existing Oracle Identity Management domain with Oracle Access Manager is extended to support Oracle Identity Manager.
29. Set up LDAP Synchronization for Oracle Identity Manager, as described in Setting Up LDAP Synchronization.
30. Verify LDAP Synchronization, as described in Verifying the LDAP Synchronization.
31. Restart the Administration Server, as described in Restarting Servers.
32. Start the Oracle Identity Manager Configuration Wizard, as described in Starting the Oracle Identity Manager 11g Configuration Wizard.
33. 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.
34. 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.

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

14.6.5 Scenario 3: Configuration in a Domain Containing OAAM, OAPM, and OIN

This section discusses the following topics:

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure

14.6.5.1 Appropriate Deployment Environment

Perform the configuration in this topic if you want to install Oracle Access Manager (OAM) in an existing Oracle Identity Management domain that contains Oracle Adaptive Access Manager (OAAM), Oracle Authorization Policy Manager (OAPM), and Oracle Identity Navigator (OIN). You can configure Oracle Access Manager to use Oracle Internet Directory (OID) as the LDAP provider. Then you can add Oracle Identity Manager (OIM) to the same domain and set up LDAP Sync.

At a later time, you may set up integration between Oracle Identity Manager and Oracle Access Manager, as described in Integration Between OIM and OAM.

You can use Oracle Identity Navigator to discover and launch Consoles for the Oracle Identity Management products from within the Oracle Identity Navigator user interface.

14.6.5.2 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

14.6.5.3 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, Oracle Adaptive Access Manager, and Oracle Access Manager. For more information, see Creating

Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU).

14.6.5.4 Procedure

Perform the following steps to configure Oracle Identity Manager with LDAP Sync to an existing Oracle Access Manager installation, which has LDAP configured:

1. Ensure that all the prerequisites, listed in Prerequisites, are satisfied. In addition, see Important Notes Before You Begin.
2. 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.
3. On the Welcome screen, select the **Create a new WebLogic domain** option. Click **Next**. The Select Domain Source screen is displayed.
4. On the Select Domain Source screen, select the following domain configuration options:
   - **Oracle Adaptive Access Manager Admin Server - 11.1.1.3.0 [Oracle_IDM2]**

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

   - **Oracle Authorization Policy Manager - 11.1.1.3.0 [Oracle_IDM2]**
5. After selecting the domain configuration options, click **Next**. The Specify Domain Name and Location screen is displayed.
6. 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.
7. 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.
8. Choose `JRockit SDK 160_17_R28.0.0-679` 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.
9. On the Configure JDBC Component Schema screen, select a component schema, such as the APM Schema, the OAAM Admin Schema, the OAAM Admin MDS Schema, or the APM 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.
10. On the Select Optional Configuration screen, you can configure **Administration Server, Managed Servers, Clusters, and Machines**, **Deployments and Services**, and **RDBMS Security 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 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.

  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.

11. On the Configuration Summary screen, review the domain configuration, and click **Create** to start creating the domain. After the domain configuration is complete, click **Done** to dismiss the wizard.

    A new WebLogic domain to support Oracle Adaptive Access Manager, Oracle Authorization Policy Manager, and Oracle Identity Navigator is created in the `<MW_HOME>\user_projects\domains` directory (on Windows), by default. On UNIX, the domain is created in the `<MW_HOME>/user_projects/domains` directory, by default.
12. 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.
13. On the Welcome screen, select the **Extend an existing WebLogic domain** option. Click **Next**. The Select a WebLogic Domain Directory screen is displayed.
14. On the Select a WebLogic Domain Directory screen, select the Oracle Identity Management domain in which you configured Oracle Adaptive Access Manager, Oracle Authorization Policy Manager, and Oracle Identity Navigator. Click **Next**. The Select Extension Source screen is displayed.
15. On the Select Extension Source screen, select the following domain configuration options:

    Oracle Access Manager with Database Policy Store - 11.1.1.3.0 [Oracle_IDM2]
16. After selecting the domain configuration options, click **Next**. The Specify Domain Name and Location screen is displayed.
17. On the Specify Domain Name and Location screen, select a location to store the applications in the domain. Click **Next**. The Configure JDBC Component Schema screen is displayed.
18. On the Configure JDBC Component Schema screen, select a component schema, such as the OAM Infrastructure Schema, the OAAM Admin Schema, the APM Schema, the APM MDS Schema, the OAAM Admin MDS Schema, that you want to modify.

You can set values for Schema Owner, Schema Password, Database and Service, Host Name, and Port. Click **Next**. The Test JDBC Component Schema screen appears. After the test succeeds, the Select Optional Configuration screen appears.

19. On the Select Optional Configuration screen, you can configure **Managed Servers, Clusters, and Machines**, and **Deployments and Services**. 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.

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

    Your existing Oracle Identity Management domain with Oracle Adaptive Access Manager, Oracle Authorization Policy Manager, and Oracle Identity Navigator is extended to support Oracle Access Manager.
21. Start the WebLogic Administration Server and Managed Servers (Oracle Identity Manager and Oracle Access Manager), as described in Starting the Stack.
22. 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=oracle,dc=com"
,ldapUrl="ldap://<oid host>:<oid port>" ,isPrimary="true"
,userIDProvider="OracleUserRoleAPI" ,
groupSearchBase="cn=Groups,dc=us,dc=oracle,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*.

23. 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.
24. On the Welcome screen, select the **Extend an existing WebLogic domain** option. Click **Next**. The Select a WebLogic Domain Directory screen is displayed.
25. On the Select a WebLogic Domain Directory screen, select the Oracle Identity Management domain in which you configured Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Authorization Policy Manager, and Oracle Identity Navigator. Click **Next**. The Select Extension Source screen is displayed.
26. 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 WSM Policy Manager - 11.1.1.0 [oracle_common]** and **Oracle SOA Suite - 11.1.1.0 [Oracle_SOA1]**

27. After selecting the domain configuration options, click **Next**. The Specify Domain Name and Location screen is displayed.
28. On the Specify Domain Name and Location screen, select a location to store the applications in the domain. Click **Next**. The Configure JDBC Component Schema screen is displayed.

29. On the Configure JDBC Component Schema screen, select a component schema, such as the SOA Infrastructure Schema, the OAM Infrastructure Schema, the OAAM Admin Schema, the User Messaging Service Schema, the OIM Schema, the OWSM MDS Schema, the OIM MDS Schema, the APM Schema, the APM MDS Schema, the OAAM Admin MDS Schema, that you want to modify.

    You can set values for Schema Owner, Schema Password, Database and Service, Host Name, and Port. Click **Next**. The Test JDBC Component Schema screen appears. After the test succeeds, the Select Optional Configuration screen appears.

30. 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.

      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.

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

    Your existing Oracle Identity Management domain with Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Authorization Policy Manager, and Oracle Identity Navigator is extended to support Oracle Identity Manager.

32. Set up LDAP Synchronization for Oracle Identity Manager, as described in Setting Up LDAP Synchronization.

33. Verify LDAP Synchronization, as described in Verifying the LDAP Synchronization.

34. Restart the Administration Server, as described in Restarting Servers.

35. Start the Oracle Identity Manager Configuration Wizard, as described in Starting the Oracle Identity Manager 11g Configuration Wizard.

36. 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.

37. Follow the wizard and the steps described in Configuring OIM Server to complete the Oracle Identity ManagerServer 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.

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

14.7 OIM with LDAP Sync in an Existing OAM and OAAM Installation with LDAP Configured

This section describes how to configure Oracle Identity Manager (OIM) with LDAP Sync to an existing Oracle Access Manager and Oracle Adaptive Access Manager installation, which has Oracle Internet Directory (OID) configured as the LDAP provider.

It contains the following sections:

- Overview
- Prerequisites
- Scenario 1: Configuration in a New WebLogic Domain
- Scenario 2: Configuration in a Domain Containing OID and OVD
- Scenario 3: Configuration in a Domain Containing OAAM, OAPM, and OIN

14.7.1 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 Access Manager and Oracle Adaptive Access Manager
3. Configure Oracle Access Manager to use Oracle Internet Directory as the LDAP provider
4. Configure Oracle Identity Manager
5. Set up LDAP sync for Oracle Identity Manager
6. Configure Oracle Identity Manager Server, Design Console (Windows only), and Remote Manager

14.7.2 Prerequisites

The following lists the prerequisites for installing and configuring Oracle Identity Manager with LDAP Synchronization to an existing Oracle Access Manager and Oracle Adaptive Access Manager installation, which has LDAP configured:

- 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 11*g* Release 1 (11.1.1.3.0) suite containing Oracle Internet Directory (OID) and Oracle Virtual Directory (OVD) are installed, as described in Installing OID, OVD, ODSM, ODIP, and OIF (11.1.1.5.0).

  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 OID and OVD with ODSM in a New WebLogic Domain.
- Install Oracle Identity Management 11*g* Release 1 (11.1.1.3.0) 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)

14.7.3 Scenario 1: Configuration in a New WebLogic Domain

This section discusses the following topics:

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure

14.7.3.1 Appropriate Deployment Environment

Perform configuration in this section for Oracle Identity Management environments that have the following conditions:

- Oracle Internet Directory, Oracle Virtual Directory, Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager are installed on the same machine.

- Oracle Access Manager and Oracle Adaptive Access Manager are configured in a new WebLogic domain, which is extended to support Oracle Identity Manager at a later time.
- Oracle Access Manager is configured to use Oracle Internet Directory as the LDAP provider before configuring LDAP Sync for Oracle Identity Manager.

14.7.3.2 Components Deployed

Performing this configuration deploys the following:

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

14.7.3.3 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, Oracle Adaptive Access Manager, and Oracle Access Manager. For more information, see Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU).

14.7.3.4 Procedure

Perform the following steps to configure Oracle Identity Manager with LDAP Synchronization, to an existing Oracle Access Manager and Oracle Adaptive Access Manager installation, which has LDAP configured:

1. Ensure that all the prerequisites, listed in Prerequisites, are satisfied. In addition, see Important Notes Before You Begin.
2. 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.
3. On the Welcome screen, select the **Create a new WebLogic domain** option. Click **Next**. The Select Domain Source screen is displayed.
4. On the Select Domain Source screen, ensure that the **Generate a domain configured automatically to support the following products:** option is selected.

   Select **Oracle Access Manager with Database Policy Store - 11.1.1.3.0 [Oracle_IDM2]** and **Oracle Adaptive Access Manager Admin Server - 11.1.1.3.0 [Oracle_IDM2]** options.

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

When you select the **Oracle Adaptive Access Manager Admin Server - 11.1.1.3.0 [Oracle_IDM1]** option, the following options are also selected, by default: **Oracle Enterprise Manager - 11.1.1.0 [oracle_common]** and **Oracle Identity Navigator - 11.1.1.3.0 [Oracle_IDM2]**

5. After selecting the domain configuration options, click **Next**. The Specify Domain Name and Location screen is displayed.
6. 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.
7. 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.
8. Choose `JRockit SDK 160_17_R28.0.0-679` 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.
9. On the Configure JDBC Component Schema screen, select a component schema, such as the OAM Infrastructure Schema, the OAAM Admin Schema, or the OAAM Admin MDS Schema, that you want to modify.

   You can set values for Schema Owner, Schema Password, Database and Service, Host Name, and Port. Click **Next**. The Test JDBC Component Schema screen appears. After the test succeeds, the Select Optional Configuration screen appears.
10. On the Select Optional Configuration screen, you can configure **Administration Server, Managed Servers, Clusters, and Machines**, **Deployments and Services**, and **RDBMS Security 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 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.

      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: Target deployments and services to servers or clusters.
- Optional: Configure RDBMS Security Store, as required.

11. 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 and Oracle Access Manager is created in the `<MW_HOME>\user_projects\domains` directory (on Windows), by default. On UNIX, the domain is created in the `<MW_HOME>/user_projects/domains` directory, by default.

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

13. 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=oracle,dc=com"
    ,ldapUrl="ldap://<oid host>:<oid port>" ,isPrimary="true"
    ,userIDProvider="OracleUserRoleAPI" ,
    groupSearchBase="cn=Groups,dc=us,dc=oracle,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*.

14. 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.
15. On the Welcome screen, select the **Extend an existing WebLogic domain** option. Click **Next**. The Select a WebLogic Domain Directory screen is displayed.
16. On the Select a WebLogic Domain Directory screen, select the Oracle Identity Management domain in which you configured Oracle Adaptive Access Manager and Oracle Access Manager. Click **Next**. The Select Extension Source screen is displayed.
17. 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]**.
18. After selecting the domain configuration options, click **Next**. The Specify Domain Name and Location screen is displayed.
19. On the Specify Domain Name and Location screen, select a location to store the applications in the domain. Click **Next**. The Configure JDBC Component Schema screen is displayed.
20. On the Configure JDBC Component Schema screen, select a component schema, such as the OAM Infrastructure Schema, the SOA Infrastructure Schema, the OAAM Admin Schema, the OAAM Admin MDS 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.
21. 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.

  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.

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

    Your existing Oracle Identity Management domain with Oracle Adaptive Access Manager and Oracle Access Manager is extended to support Oracle Identity Manager.

23. Set up LDAP Synchronization for Oracle Identity Manager, as described in Setting Up LDAP Synchronization.
24. Verify LDAP Synchronization, as described in Verifying the LDAP Synchronization.
25. Restart the Administration Server, as described in Restarting Servers.
26. Start the Oracle Identity Manager Configuration Wizard, as described in Starting the Oracle Identity Manager 11g Configuration Wizard.
27. 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.
28. Follow the wizard and the steps described in Configuring OIM Server to complete the Oracle Identity ManagerServer 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.

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

14.7.4 Scenario 2: Configuration in a Domain Containing OID and OVD

This section discusses the following topics:

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure

14.7.4.1 Appropriate Deployment Environment

Perform configuration in this section for Oracle Identity Management environments that have the following conditions:

- Oracle Internet Directory, Oracle Virtual Directory, Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager are installed on the same machine.
- Oracle Access Manager and Oracle Adaptive Access Manager are configured in the existing Oracle Identity Management domain containing Oracle Internet Directory and Oracle Virtual Directory. This domain is extended to support Oracle Identity Manager at a later time.
- Oracle Access Manager is configured to use Oracle Internet Directory as the LDAP provider before configuring LDAP Sync for Oracle Identity Manager.

14.7.4.2 Components Deployed

Performing this configuration deploys the following:

- Managed Servers for Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager
- Oracle Access Manager Console and Oracle Adaptive Access Manager Console on the existing Administration Server
- Oracle Identity Administration Console, Oracle Identity Manager Self Service Console, and Oracle Identity Manager Advanced Administration Console on the Oracle Identity Manager Managed Server

14.7.4.3 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, Oracle Adaptive Access Manager, and Oracle Access Manager. For more information, see Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU).

14.7.4.4 Procedure

Perform the following steps to configure Oracle Identity Manager with LDAP Synchronization, to an existing Oracle Access Manager and Oracle Adaptive Access Manager installation, which has LDAP configured:

1. Ensure that all the prerequisites, listed in Prerequisites, are satisfied. In addition, see Important Notes Before You Begin.
2. 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.

3. On the Select Domain screen, select the **Create New Domain** option. Set the Administrator user name and password, as required.
4. Ensure that you select **Oracle Internet Directory** and **Oracle Virtual Directory** on the Configure Components screen.
5. 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.
6. Ensure that your Oracle database version is supported and you have installed the necessary patches. For more information, see Installing Oracle Database.
7. 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).
8. 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.
9. 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.
10. 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.
11. On the Welcome screen, select the **Extend an existing WebLogic domain** option. Click **Next**. The Select a WebLogic Domain Directory screen is displayed.
12. 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.
13. On the Select Extension Source screen, select the following domain configuration options:

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

    Oracle Adaptive Access Manager Admin Server - 11.1.1.3.0 [Oracle_IDM2]

    > **Note:** When you select the **Oracle Adaptive Access Manager Admin Server - 11.1.1.3.0 [Oracle_IDM2]** option, the **Oracle Identity Navigator - 11.1.1.3.0 [Oracle_IDM2]** option is also selected, by default.

14. After selecting the domain configuration options, click **Next**. The Configure JDBC Component Schema screen is displayed.
15. On the Configure JDBC Component Schema screen, select a component schema, such as the OAM Infrastructure Schema, the OAAM Admin Schema, or the OAAM Admin MDS Schema, that you want to modify.

You can set values for Schema Owner, Schema Password, Database and Service, Host Name, and Port. Click **Next**. The Test JDBC Component Schema screen appears. After the test succeeds, the Select Optional Configuration screen appears.

16. On the Select Optional Configuration screen, you can configure **Managed Servers, Clusters, and Machines**, **Deployments and Services**. 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.

      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.
17. 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 Access Manager and Oracle Adaptive Access Manager.
18. Start the WebLogic Administration Server and Managed Servers (Oracle Identity Manager and Oracle Access Manager), as described in Starting the Stack.
19. 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=oracle,dc=com"
,ldapUrl="ldap://<oid host>:<oid port>" ,isPrimary="true"
,userIDProvider="OracleUserRoleAPI" ,
groupSearchBase="cn=Groups,dc=us,dc=oracle,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*.

20. 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.
21. On the Welcome screen, select the **Extend an existing WebLogic domain** option. Click **Next**. The Select a WebLogic Domain Directory screen is displayed.
22. On the Select a WebLogic Domain Directory screen, select the Oracle Identity Management domain in which you configured Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Internet Directory and Oracle Virtual Directory. Click **Next**. The Select Extension Source screen is displayed.
23. 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]**.
24. After selecting the domain configuration options, click **Next**. The Specify Domain Name and Location screen is displayed.
25. On the Specify Domain Name and Location screen, select a location to store the applications in the domain. Click **Next**. The Configure JDBC Component Schema screen is displayed.

26. 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 OAAM Admin Schema, the OAAM Admin 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.

27. 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.

      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.

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

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

29. Set up LDAP Synchronization for Oracle Identity Manager, as described in Setting Up LDAP Synchronization.

30. Verify LDAP Synchronization, as described in Verifying the LDAP Synchronization.

31. Restart the Administration Server, as described in Restarting Servers.

32. Start the Oracle Identity Manager Configuration Wizard, as described in Starting the Oracle Identity Manager 11g Configuration Wizard.

33. 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.

34. Follow the wizard and the steps described in Configuring OIM Server to complete the Oracle Identity ManagerServer 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.

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

14.7.5 Scenario 3: Configuration in a Domain Containing OAPM, and OIN

This section discusses the following topics:

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure

14.7.5.1 Appropriate Deployment Environment

Perform configuration in this section for Oracle Identity Management environments that have the following conditions:

- Oracle Internet Directory, Oracle Virtual Directory, Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager are installed on the same machine.
- Oracle Access Manager and Oracle Adaptive Access Manager are configured in the existing Oracle Identity Management domain containing Oracle Authorization Policy Manager and Oracle Identity Navigator. This domain is extended to support Oracle Identity Manager at a later time.
- Oracle Access Manager is configured to use Oracle Internet Directory as the LDAP provider before configuring LDAP Sync for Oracle Identity Manager.

14.7.5.2 Components Deployed

Performing the configuration in this section deploys the following:

- Managed Servers for Oracle Identity Manager, Oracle Adaptive Access 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 and Oracle Adaptive Access Manager Console on the existing Administration Server

14.7.5.3 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, Oracle Adaptive Access Manager, and Oracle Access Manager. For more information, see Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU).

14.7.5.4 Procedure

Perform the following steps to configure Oracle Identity Manager with LDAP Sync to an existing Oracle Access Manager and Oracle Adaptive Access Manager installation, which has LDAP configured:

1. Ensure that all the prerequisites, listed in Prerequisites, are satisfied. In addition, see Important Notes Before You Begin.
2. 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.
3. On the Welcome screen, select the **Create a new WebLogic domain** option. Click **Next**. The Select Domain Source screen is displayed.
4. On the Select Domain Source screen, select the following domain configuration options:
   - **Oracle Authorization Policy Manager - 11.1.1.3.0 [Oracle_IDM2]**

     Note: When you select the **Oracle Authorization Policy Manager - 11.1.1.3.0 [Oracle_IDM2]** option, the **Oracle JRF - 11.1.1.0 [oracle_common]** option is also selected, by default.

   - **Oracle Identity Navigator - 11.1.1.3.0 [Oracle_IDM2]**
5. After selecting the domain configuration options, click **Next**. The Specify Domain Name and Location screen is displayed.
6. 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.
7. 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.
8. Choose `JRockit SDK 160_17_R28.0.0-679` 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.
9. On the Configure JDBC Component Schema screen, select a component schema, such as the APM Schema, or the APM 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.

10. On the Select Optional Configuration screen, you can configure **Administration Server, Managed Servers, Clusters, and Machines**, **Deployments and Services**, and **RDBMS Security 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 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.

      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.
11. On the Configuration Summary screen, review the domain configuration, and click **Create** to start creating the domain. After the domain configuration is complete, click **Done** to dismiss the wizard.

    A new WebLogic domain to support Oracle Authorization Policy Manager and Oracle Identity Navigator is created in the `<MW_HOME>\user_projects\domains` directory (on Windows), by default. On UNIX, the domain is created in the `<MW_HOME>/user_projects/domains` directory, by default.
12. 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.
13. On the Welcome screen, select the **Extend an existing WebLogic domain** option. Click **Next**. The Select a WebLogic Domain Directory screen is displayed.
14. On the Select a WebLogic Domain Directory screen, select the Oracle Identity Management domain in which you configured Oracle Authorization Policy Manager, and Oracle Identity Navigator. Click **Next**. The Select Extension Source screen is displayed.
15. On the Select Extension Source screen, select the following domain configuration options:

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

    Oracle Adaptive Access Manager Admin Server - 11.1.1.3.0 [Oracle_IDM2]

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

16. After selecting the domain configuration options, click **Next**. The Specify Domain Name and Location screen is displayed.
17. On the Specify Domain Name and Location screen, select a location to store the applications in the domain. Click **Next**. The Configure JDBC Component Schema screen is displayed.
18. On the Configure JDBC Component Schema screen, select a component schema, such as the OAM Infrastructure Schema, the OAAM Admin Schema, the APM Schema, the APM MDS Schema, the OAAM Admin MDS Schema, that you want to modify.

    You can set values for Schema Owner, Schema Password, Database and Service, Host Name, and Port. Click **Next**. The Test JDBC Component Schema screen appears. After the test succeeds, the Select Optional Configuration screen appears.
19. On the Select Optional Configuration screen, you can configure **Managed Servers, Clusters, and Machines**, and **Deployments and Services**. 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.

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

    Your existing Oracle Identity Management domain with Oracle Authorization Policy Manager and Oracle Identity Navigator is extended to support Oracle Access Manager and Oracle Adaptive Access Manager.
21. Start the WebLogic Administration Server and Managed Servers (Oracle Identity Manager and Oracle Access Manager), as described in Starting the Stack.

22. 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=oracle,dc=com"
    ,ldapUrl="ldap://<oid host>:<oid port>" ,isPrimary="true"
    ,userIDProvider="OracleUserRoleAPI" ,
    groupSearchBase="cn=Groups,dc=us,dc=oracle,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*.

23. 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.

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

25. On the Select a WebLogic Domain Directory screen, select the Oracle Identity Management domain in which you configured Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Authorization Policy Manager, and Oracle Identity Navigator. Click **Next**. The Select Extension Source screen is displayed.
26. 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 WSM Policy Manager - 11.1.1.0 [oracle_common]** and **Oracle SOA Suite - 11.1.1.0 [Oracle_SOA1]**

27. After selecting the domain configuration options, click **Next**. The Specify Domain Name and Location screen is displayed.
28. On the Specify Domain Name and Location screen, select a location to store the applications in the domain. Click **Next**. The Configure JDBC Component Schema screen is displayed.
29. On the Configure JDBC Component Schema screen, select a component schema, such as the SOA Infrastructure Schema, the OAM Infrastructure Schema, the OAAM Admin Schema, the User Messaging Service Schema, the OIM Schema, the OWSM MDS Schema, the OIM MDS Schema, the APM Schema, the APM MDS Schema, the OAAM Admin MDS Schema, that you want to modify.

    You can set values for Schema Owner, Schema Password, Database and Service, Host Name, and Port. Click **Next**. The Test JDBC Component Schema screen appears. After the test succeeds, the Select Optional Configuration screen appears.
30. 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.

      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.

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

    Your existing Oracle Identity Management domain with Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Authorization Policy Manager, and Oracle Identity Navigator is extended to support Oracle Identity Manager.

32. Set up LDAP Synchronization for Oracle Identity Manager, as described in Setting Up LDAP Synchronization.

33. Verify LDAP Synchronization, as described in Verifying the LDAP Synchronization.

34. Restart the Administration Server, as described in Restarting Servers.

35. Start the Oracle Identity Manager Configuration Wizard, as described in Starting the Oracle Identity Manager 11g Configuration Wizard.

36. 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.

37. Follow the wizard and the steps described in Configuring OIM Server to complete the Oracle Identity ManagerServer 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.

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

14.8 OAM in an Existing OIM with LDAP Sync

This section describes how to add Oracle Access Manager to an existing Oracle Identity Manager (OIM) installation, which has LDAP Sync configured. It also describes how to configure Oracle Access Manager to use Oracle Internet Directory (OID) as its LDAP provider.

It contains the following sections:

- Overview
- Prerequisites
- Scenario 1: Configuration in a New WebLogic Domain
- Scenario 2: Configuration in a Domain Containing OID and OVD
- Scenario 3: Configuration in a Domain Containing OAAM, OAPM, and OIN

14.8.1 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

3. Set up LDAP Sync for Oracle Identity Manager
4. Configure Oracle Access Manager
5. Configure Oracle Access Manager to use Oracle Internet Directory as the LDAP provider
6. Configure Oracle Identity Manager Server, Design Console (Windows only), and Remote Manager

14.8.2 Prerequisites

The following lists the prerequisites for installing and configuring Oracle Identity Manager with LDAP Synchronization to an existing Oracle Access Manager and Oracle Adaptive Access Manager installation, which has LDAP configured:

- 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 11*g* Release 1 (11.1.1.3.0) suite containing Oracle Internet Directory (OID) and Oracle Virtual Directory (OVD) are installed, as described in Installing OID, OVD, ODSM, ODIP, and OIF (11.1.1.5.0).

  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 OID and OVD with ODSM in a New WebLogic Domain.
- Install Oracle Identity Management 11*g* Release 1 (11.1.1.3.0) 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)

14.8.3 Scenario 1: Configuration in a New WebLogic Domain

This section discusses the following topics:

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure

14.8.3.1 Appropriate Deployment Environment

Perform configuration in this section for Oracle Identity Management environments that have the following conditions:

- Oracle Internet Directory, Oracle Virtual Directory, Oracle Access Manager, and Oracle Identity Manager are installed on the same machine.
- Oracle Identity Manager is configured in a new WebLogic domain, which is extended to support Oracle Access Manager at a later time.
- Oracle Access Manager is configured to use Oracle Internet Directory as the LDAP provider after configuring LDAP Sync for Oracle Identity Manager.

14.8.3.2 Components Deployed

Performing this configuration deploys the following:

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

14.8.3.3 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).

14.8.3.4 Procedure

Perform the following steps to configure Oracle Access Manager to an existing Oracle Identity Manager installation with LDAP Sync:

1. Ensure that all the prerequisites, listed in Prerequisites, are satisfied. In addition, see Important Notes Before You Begin.

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

   Select **Oracle Identity Manager - 11.1.1.3.0 [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 JRF 11.1.1.0 [Oracle_Common], **Oracle Enterprise Manager - 11.1.1.0 [oracle_common]**, **Oracle WSM Policy Manager - 11.1.1.0 [oracle_common]**, and **Oracle SOA Suite - 11.1.1.0 [Oracle_SOA1]**.

   ---

5. After selecting the domain configuration options, click **Next**. The Specify Domain Name and Location screen is displayed.
6. 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.
7. 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.
8. Choose `JRockit SDK 160_17_R28.0.0-679` 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.
9. On the Configure JDBC Component Schema screen, select a component schema, such as the SOA Infrastructure Schema, the User Messaging Service Schema, the OIM MDS Schema, the OWSM MDS Schema, the SOA MDS Schema, or the OIM 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.
10. On the Select Optional Configuration screen, you can configure **Administration Server, Managed Servers, Clusters, and Machines**, **Deployments and Services**, **JMS File Store**, and **RDBMS Security 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 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.

  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: Target deployments and services to servers or clusters.
- Optional: Configure JMS File Store, as required.
- Optional: Configure RDBMS Security Store, as required.

11. 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 is created in the `<MW_HOME>\user_projects\domains` directory (on Windows), by default. On UNIX, the domain is created in the `<MW_HOME>/user_projects/domains` directory, by default.

12. Set up LDAP Synchronization for Oracle Identity Manager, as described in Setting Up LDAP Synchronization.

13. Verify LDAP Synchronization, as described in Verifying the LDAP Synchronization.

14. 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.

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

16. On the Select a WebLogic Domain Directory screen, select the Oracle Identity Management domain in which you configured Oracle Identity Manager. Click **Next**. The Select Extension Source screen is displayed.

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

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

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

19. On the Specify Domain Name and Location screen, select a location to store the applications in the domain. Click **Next**. The Configure JDBC Component Schema screen is displayed.

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

21. 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.

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

    Your existing Oracle Identity Management domain with Oracle Identity Manager is extended to support Oracle Access Manager.
23. Start the WebLogic Administration Server and Managed Servers (Oracle Identity Manager and Oracle Access Manager), as described in Starting the Stack.
24. 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=oracle,dc=com"
,ldapUrl="ldap://<oid host>:<oid port>" ,isPrimary="true"
,userIDProvider="OracleUserRoleAPI" ,
groupSearchBase="cn=Groups,dc=us,dc=oracle,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*.

25. Start the Oracle Identity Manager Configuration Wizard, as described in Starting the Oracle Identity Manager 11g Configuration Wizard.
26. 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.
27. 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.

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

14.8.4 Scenario 2: Configuration in a Domain Containing OID and OVD

This section discusses the following topics:

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure

14.8.4.1 Appropriate Deployment Environment

Perform configuration in this section for Oracle Identity Management environments that have the following conditions:

- Oracle Internet Directory, Oracle Virtual Directory, Oracle Access Manager, and Oracle Identity Manager are installed on the same machine.
- Oracle Identity Manager is configured in the existing Oracle Identity Management domain containing Oracle Internet Directory and Oracle Virtual Directory. This domain is extended to support Oracle Access Manager at a later time.
- Oracle Access Manager is configured to use Oracle Internet Directory as the LDAP provider after configuring LDAP Sync for Oracle Identity Manager.

14.8.4.2 Components Deployed

Performing this configuration deploys the following:

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

14.8.4.3 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).

14.8.4.4 Procedure

Perform the following steps to configure Oracle Access Manager to an existing Oracle Identity Manager installation, which has LDAP Sync set up:

1. Ensure that all the prerequisites, listed in Prerequisites, are satisfied. In addition, see Important Notes Before You Begin.
2. 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.
3. On the Select Domain screen, select the **Create New Domain** option. Set the Administrator user name and password, as required.
4. Ensure that you select **Oracle Internet Directory** and **Oracle Virtual Directory** on the Configure Components screen.
5. 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.

6. Ensure that your Oracle database version is supported and you have installed the necessary patches. For more information, see Installing Oracle Database.
7. 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).
8. 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.
9. 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.
10. 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.
11. On the Welcome screen, select the **Extend an existing WebLogic domain** option. Click **Next**. The Select a WebLogic Domain Directory screen is displayed.
12. 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.
13. 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 **Oracle WSM Policy Manager - 11.1.1.0 [oracle_common]** option and the **Oracle SOA Suite - 11.1.1.3.0 [Oracle_SOA1]** option are also selected, by default.

14. After selecting the domain configuration options, click **Next**. The Configure JDBC Component Schema screen is displayed.
15. On the Configure JDBC Component Schema screen, select a component schema, such as the SOA Infrastructure Schema, the User Messaging Service Schema, the OIM MDS Schema, the OWSM 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.
16. 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.

  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.

17. 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.
18. Set up LDAP Synchronization for Oracle Identity Manager, as described in Setting Up LDAP Synchronization.
19. Verify LDAP Synchronization, as described in Verifying the LDAP Synchronization.
20. 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.
21. On the Welcome screen, select the **Extend an existing WebLogic domain** option. Click **Next**. The Select a WebLogic Domain Directory screen is displayed.
22. On the Select a WebLogic Domain Directory screen, select the Oracle Identity Management domain in which you configured Oracle Identity Manager, Oracle Internet Directory, and Oracle Virtual Directory. Click **Next**. The Select Extension Source screen is displayed.
23. On the Select Extension Source screen, select the following domain configuration options:

    Oracle Access Manager with Database Policy Store - 11.1.1.3.0 [Oracle_IDM2]
24. After selecting the domain configuration options, click **Next**. The Specify Domain Name and Location screen is displayed.
25. On the Specify Domain Name and Location screen, select a location to store the applications in the domain. Click **Next**. The Configure JDBC Component Schema screen is displayed.
26. On the Configure JDBC Component Schema screen, select a component schema, such as the SOA Infrastructure Schema, the OAM Infrastructure Schema, the User

Messaging Service Schema, the OIM MDS Schema, the OWSM 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.

27. 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.

      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.

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

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

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

30. 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=oracle,dc=com"
,ldapUrl="ldap://<oid host>:<oid port>" ,isPrimary="true"
,userIDProvider="OracleUserRoleAPI" ,
groupSearchBase="cn=Groups,dc=us,dc=oracle,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*.

31. Restart the Administration Server, as described in Restarting Servers.
32. Start the Oracle Identity Manager Configuration Wizard, as described in Starting the Oracle Identity Manager 11g Configuration Wizard.
33. 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.
34. 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.

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

14.8.5 Scenario 3: Configuration in a Domain Containing OAPM, and OIN

This section discusses the following topics:

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure

14.8.5.1 Appropriate Deployment Environment

Perform configuration in this section for Oracle Identity Management environments that have the following conditions:

- Oracle Internet Directory, Oracle Virtual Directory, Oracle Access Manager, and Oracle Identity Manager are installed on the same machine.
- Oracle Identity Manager is configured in the existing Oracle Identity Management domain containing Oracle Authorization Policy Manager, Oracle Adaptive Access Manager, and Oracle Identity Navigator. This domain is extended to support Oracle Access Manager at a later time.
- Oracle Access Manager is configured to use Oracle Internet Directory as the LDAP provider after configuring LDAP Sync for Oracle Identity Manager.

14.8.5.2 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

14.8.5.3 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, Oracle Adaptive Access Manager, and Oracle Access Manager. For more information, see Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU).

14.8.5.4 Procedure

Perform the following steps to configure Oracle Access Manager in an existing Oracle Identity Manager with LDAP Sync installation:

1. Ensure that all the prerequisites, listed in Prerequisites, are satisfied. In addition, see Important Notes Before You Begin.
2. 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.
3. On the Welcome screen, select the **Create a new WebLogic domain** option. Click **Next**. The Select Domain Source screen is displayed.
4. On the Select Domain Source screen, select the following domain configuration options:

   Oracle Authorization Policy Manager - 11.1.1.3.0 [Oracle_IDM2]

   Oracle Adaptive Access Manager Admin Server - 11.1.1.3.0 [Oracle_IDM2]

   Oracle Identity Manager - 11.1.1.3.0 [Oracle_IDM2]

   Note: When you select the **Oracle Authorization Policy Manager - 11.1.1.3.0 [Oracle_IDM2]** option, the **Oracle JRF - 11.1.1.0 [oracle_common]** option is also selected, by default.

   When you select the **Oracle Adaptive Access Manager Admin Server - 11.1.1.3.0 [Oracle_IDM2]** option, the **Oracle Identity Navigator - 11.1.1.3.0 [Oracle_IDM2]** option is also selected, by default.

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

   ---

5. After selecting the domain configuration options, click **Next**. The Specify Domain Name and Location screen is displayed.
6. 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.
7. 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.
8. Choose `JRockit SDK 160_17_R28.0.0-679` 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.
9. On the Configure JDBC Component Schema screen, select a component schema, such as the APM Schema, the SOA Infrastructure Schema, the SOA MDS Schema, the OIM MDS Schema, the OIM Schema, the OAAM Admin Schema, the OAAM Admin MDS Schema, the OWSM MDS Schema, the User Messaging Service Schema, or the APM 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.

10. On the Select Optional Configuration screen, you can configure **Administration Server, Managed Servers, Clusters, and Machines**, **Deployments and Services**, **JMS File Store**, and **RDBMS Security 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 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.

      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.
    - Optional: Configure RDBMS Security Store, as required.
11. On the Configuration Summary screen, review the domain configuration, and click **Create** to start creating the domain. After the domain configuration is complete, click **Done** to dismiss the wizard.

    A new WebLogic domain to support Oracle Authorization Policy Manager, Oracle Identity Manager, Oracle Adaptive Access Manager, and Oracle Identity Navigator is created in the `<MW_HOME>\user_projects\domains` directory (on Windows), by default. On UNIX, the domain is created in the `<MW_HOME>/user_projects/domains` directory, by default.
12. Set up LDAP Synchronization for Oracle Identity Manager, as described in Setting Up LDAP Synchronization.
13. Verify LDAP Synchronization, as described in Verifying the LDAP Synchronization.
14. 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.
15. On the Welcome screen, select the **Extend an existing WebLogic domain** option. Click **Next**. The Select a WebLogic Domain Directory screen is displayed.
16. On the Select a WebLogic Domain Directory screen, select the Oracle Identity Management domain in which you configured Oracle Identity Manager, Oracle Authorization Policy Manager, Oracle Adaptive Access Manager, and Oracle Identity Navigator. Click **Next**. The Select Extension Source screen is displayed.

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

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

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

19. On the Specify Domain Name and Location screen, select a location to store the applications in the domain. Click **Next**. The Configure JDBC Component Schema screen is displayed.

20. On the Configure JDBC Component Schema screen, select a component schema, such as the APM Schema, the OAM Infrastructure Schema, the SOA Infrastructure Schema, the SOA MDS Schema, the OIM MDS Schema, the OIM Schema, the OAAM Admin Schema, the OAAM Admin MDS Schema, the OWSM MDS Schema, the User Messaging Service Schema, or the APM 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.

21. 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.

      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.

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

    Your existing Oracle Identity Management domain with Oracle Identity Manager, Oracle Authorization Policy Manager, Oracle Adaptive Access Manager, and Oracle Identity Navigator is extended to support Oracle Access Manager.

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

24. 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=oracle,dc=com"
    ,ldapUrl="ldap://<oid host>:<oid port>" ,isPrimary="true"
    ,userIDProvider="OracleUserRoleAPI" ,
    groupSearchBase="cn=Groups,dc=us,dc=oracle,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*.

25. Start the Oracle Identity Manager Configuration Wizard, as described in Starting the Oracle Identity Manager 11g Configuration Wizard.

26. 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.

27. Follow the wizard and the steps described in Configuring OIM Server to complete the Oracle Identity ManagerServer 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.

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

14.9 OAAM in an Existing OIM with LDAP Sync and OAAM

This section describes how to add Oracle Adaptive Access Manager to an existing Oracle Access Manager and Oracle Identity Manager (OIM) installation, which has LDAP Sync configured. It also describes how to configure Oracle Access Manager to use Oracle Internet Directory (OID) as its LDAP provider.

It contains the following sections:

- Overview
- Prerequisites
- Scenario 1: Configuration in a New WebLogic Domain
- Scenario 2: Configuration in a Domain Containing OID and OVD
- Scenario 3: Configuration in a Domain Containing OAAM, OAPM, and OIN

14.9.1 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

14.9.2 Prerequisites

The following lists the prerequisites for installing and configuring Oracle Adaptive Access Manager to an existing Oracle Access Manager Oracle Identity Manager installation with LDAP sync:

- 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 11*g* Release 1 (11.1.1.3.0) suite containing Oracle Internet Directory (OID) and Oracle Virtual Directory (OVD) are installed, as described in Installing OID, OVD, ODSM, ODIP, and OIF (11.1.1.5.0).

  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 OID and OVD with ODSM in a New WebLogic Domain.
- Install Oracle Identity Management 11*g* Release 1 (11.1.1.3.0) 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)

14.9.3 Scenario 1: Configuration in a New WebLogic Domain

This section discusses the following topics:

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure

14.9.3.1 Appropriate Deployment Environment

Perform configuration in this section for Oracle Identity Management environments that have the following conditions:

- Oracle Internet Directory, Oracle Virtual Directory, Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager are installed on the same machine.
- Oracle Identity Manager and Oracle Access Manager are configured in a new WebLogic domain, which is extended to support Oracle Adaptive Access Manager at a later time.

- Oracle Access Manager is configured to use Oracle Internet Directory as the LDAP provider after configuring LDAP Sync for Oracle Identity Manager.

14.9.3.2 Components Deployed

Performing this configuration deploys the following:

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

14.9.3.3 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, Oracle Adaptive Access Manager, and Oracle Access Manager. For more information, see Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU).

14.9.3.4 Procedure

Perform the following steps to configure Oracle Adaptive Access Manager to an existing Oracle Access Manager and Oracle Identity Manager installation with LDAP Sync:

1. Ensure that all the prerequisites, listed in Prerequisites, are satisfied. In addition, see Important Notes Before You Begin.
2. 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.
3. On the Welcome screen, select the **Create a new WebLogic domain** option. Click **Next**. The Select Domain Source screen is displayed.
4. On the Select Domain Source screen, ensure that the **Generate a domain configured automatically to support the following products:** option is selected.

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

   Select **Oracle Access Manager with Database Policy Store - 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 JRF 11.1.1.0 [Oracle_Common], **Oracle Enterprise Manager - 11.1.1.0 [oracle_common]**, **Oracle WSM Policy Manager - 11.1.1.0 [oracle_common]**, and **Oracle SOA Suite - 11.1.1.0 [Oracle_SOA1]**.

5. After selecting the domain configuration options, click **Next**. The Specify Domain Name and Location screen is displayed.
6. 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.
7. 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.
8. Choose `JRockit SDK 160_17_R28.0.0-679` 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.
9. On the Configure JDBC Component Schema screen, select a component schema, such as the SOA Infrastructure Schema, the User Messaging Service Schema, the OIM MDS Schema, the OWSM MDS Schema, the SOA MDS Schema, the OAM Infrastructure Schema, or the OIM 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.
10. On the Select Optional Configuration screen, you can configure **Administration Server, Managed Servers, Clusters, and Machines**, **Deployments and Services**, **JMS File Store**, and **RDBMS Security 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 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.

      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: Target deployments and services to servers or clusters.
- Optional: Configure JMS File Store, as required.
- Optional: Configure RDBMS Security Store, as required.

11. 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), by default. On UNIX, the domain is created in the `<MW_HOME>/user_projects/domains` directory, by default.

12. Set up LDAP Synchronization for Oracle Identity Manager, as described in Setting Up LDAP Synchronization.

13. Verify LDAP Synchronization, as described in Verifying the LDAP Synchronization.

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

15. 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=oracle,dc=com"
       ,ldapUrl="ldap://<oid host>:<oid port>" ,isPrimary="true"
       ,userIDProvider="OracleUserRoleAPI" ,
       groupSearchBase="cn=Groups,dc=us,dc=oracle,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*.

16. 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.
17. On the Welcome screen, select the **Extend an existing WebLogic domain** option. Click **Next**. The Select a WebLogic Domain Directory screen is displayed.
18. On the Select a WebLogic Domain Directory screen, select the Oracle Identity Management domain in which you configured Oracle Identity Manager and Oracle Access Manager. Click **Next**. The Select Extension Source screen is displayed.
19. On the Select Extension Source screen, select the following domain configuration options:

    Oracle Adaptive Access Manager Admin Server - 11.1.1.3.0 [Oracle_IDM2]

    > **Note:** When you select the **Oracle Adaptive Access Manager Admin Server - 11.1.1.3.0 [Oracle_IDM2]** option, the **Oracle Identity Navigator - 11.1.1.3.0 [Oracle_IDM2]** option is also selected, by default.

20. After selecting the domain configuration options, click **Next**. The Configure JDBC Component Schema screen is displayed.
21. On the Configure JDBC Component Schema screen, select a component schema, such as the SOA Infrastructure Schema, the OAM Infrastructure Schema, the User Messaging Service Schema, the OAAM Admin Schema, the OAAM Admin MDS Schema, the OIM MDS Schema, the OWSM MDS Schema, the SOA MDS Schema, or the OIM 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.
22. 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.

  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.

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

    Your existing Oracle Identity Management domain with Oracle Identity Manager and Oracle Access Manager is extended to support Oracle Adaptive Access Manager.

24. Start the Oracle Identity Manager Configuration Wizard, as described in Starting the Oracle Identity Manager 11g Configuration Wizard.
25. 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.
26. Follow the wizard and the steps described in Configuring OIM Server to complete the Oracle Identity ManagerServer 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.

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

14.9.4 Scenario 2: Configuration in a Domain Containing OID and OVD

This section discusses the following topics:

- Appropriate Deployment Environment
- Components Deployed
- Dependencies

- Procedure

14.9.4.1 Appropriate Deployment Environment

Perform configuration in this section for Oracle Identity Management environments that have the following conditions:

- Oracle Internet Directory, Oracle Virtual Directory, Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager are installed on the same machine.
- Oracle Identity Manager and Oracle Access Manager are configured in the existing Oracle Identity Management domain containing Oracle Internet Directory and Oracle Virtual Directory. This domain is extended to support Oracle Adaptive Access Manager at a later time.
- Oracle Access Manager is configured to use Oracle Internet Directory as the LDAP provider after configuring LDAP Sync for Oracle Identity Manager.

14.9.4.2 Components Deployed

Performing this configuration deploys the following:

- Managed Servers for Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager
- Oracle Access Manager Console and Oracle Adaptive Access Manager Console on the existing Administration Server
- Oracle Identity Administration Console, Oracle Identity Manager Self Service Console, and Oracle Identity Manager Advanced Administration Console on the Oracle Identity Manager Managed Server

14.9.4.3 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, Oracle Adaptive Access Manager, and Oracle Access Manager. For more information, see Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU).

14.9.4.4 Procedure

Perform the following steps to configure Oracle Adaptive Access Manager in an existing Oracle Identity Management installation, which has Oracle Internet Directory, Oracle Access Manager, Oracle Identity Manager, and Oracle Virtual Directory configured:

1. Ensure that all the prerequisites, listed in Prerequisites, are satisfied. In addition, see Important Notes Before You Begin.

2. 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.
3. On the Select Domain screen, select the **Create New Domain** option. Set the Administrator user name and password, as required.
4. Ensure that you select **Oracle Internet Directory** and **Oracle Virtual Directory** on the Configure Components screen.
5. 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.
6. Ensure that your Oracle database version is supported and you have installed the necessary patches. For more information, see Installing Oracle Database.
7. Ensure that any appropriate schemas required by Oracle Identity Manager, Oracle SOA Suite, Oracle Adaptive Access Manager, and Oracle Access Manager are created and loaded, as described in Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU).
8. 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.
9. 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.
10. 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.
11. On the Welcome screen, select the **Extend an existing WebLogic domain** option. Click **Next**. The Select a WebLogic Domain Directory screen is displayed.
12. 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.
13. On the Select Extension Source screen, select the following domain configuration options:

    Oracle Identity Manager - 11.1.1.3.0 [Oracle_IDM2]

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

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

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

15. On the Configure JDBC Component Schema screen, select a component schema, such as the SOA Infrastructure Schema, the User Messaging Service Schema, the OIM MDS Schema, the OAM Infrastructure Schema, the OWSM 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.

16. 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.

      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.

17. 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.

18. Set up LDAP Synchronization for Oracle Identity Manager, as described in Setting Up LDAP Synchronization.

19. Verify LDAP Synchronization, as described in Verifying the LDAP Synchronization.

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

21. 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=oracle,dc=com"
,ldapUrl="ldap://<oid host>:<oid port>" ,isPrimary="true"
,userIDProvider="OracleUserRoleAPI" ,
groupSearchBase="cn=Groups,dc=us,dc=oracle,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*.

22. 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.

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

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

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

Oracle Adaptive Access Manager Admin Server - 11.1.1.3.0 [Oracle_IDM2]

Note: When you select the **Oracle Adaptive Access Manager Admin Server - 11.1.1.3.0 [Oracle_IDM2]** option, the **Oracle Identity Navigator - 11.1.1.3.0 [Oracle_IDM2]** option is also selected, by default.

---

26. After selecting the domain configuration options, click **Next**. The Specify Domain Name and Location screen is displayed.
27. On the Specify Domain Name and Location screen, select a location to store the applications in the domain. Click **Next**. The Configure JDBC Component Schema screen is displayed.
28. On the Configure JDBC Component Schema screen, select a component schema, such as the SOA Infrastructure Schema, the OAAM Admin Schema, the OAAM Admin MDS Schema, the OAM Infrastructure Schema, the User Messaging Service Schema, the OIM MDS Schema, the OWSM 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.
29. 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.

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

    Your existing Oracle Identity Management domain with Oracle Identity Manager, Oracle Access Manager, Oracle Internet Directory, and Oracle Virtual Directory is extended to support Oracle Adaptive Access Manager.
31. Restart the Administration Server, as described in Restarting Servers.

32. Start the Oracle Identity Manager Configuration Wizard, as described in Starting the Oracle Identity Manager 11g Configuration Wizard.
33. 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.
34. Follow the wizard and the steps described in Configuring OIM Server to complete the Oracle Identity ManagerServer 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.

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

14.9.5 Scenario 3: Configuration in a Domain Containing OAPM, and OIN

This section discusses the following topics:

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure

14.9.5.1 Appropriate Deployment Environment

Perform configuration in this section for Oracle Identity Management environments that have the following conditions:

- Oracle Internet Directory, Oracle Virtual Directory, Oracle Adaptive Access Manager, Oracle Access Manager, and Oracle Identity Manager are installed on the same machine.
- Oracle Identity Manager and Oracle Access Manager are configured in the existing Oracle Identity Management domain containing Oracle Authorization Policy Manager, and Oracle Identity Navigator. This domain is extended to support Oracle Adaptive Access Manager at a later time.
- Oracle Access Manager is configured to use Oracle Internet Directory as the LDAP provider after configuring LDAP Sync for Oracle Identity Manager.

14.9.5.2 Components Deployed

Performing the configuration in this section deploys the following:

- Managed Servers for Oracle Identity Manager, Oracle Adaptive Access 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 and Oracle Adaptive Access Manager Console on the existing Administration Server

14.9.5.3 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, Oracle Adaptive Access Manager, and Oracle Access Manager. For more information, see Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU).

14.9.5.4 Procedure

Perform the following steps to configure Oracle Adaptive Access Manager in an existing Oracle Identity Management installation, which has Oracle Identity Manager with LDAP Sync, Oracle Access Manager, Oracle Authorization Policy Manager, and Oracle Identity Navigator:

1. Ensure that all the prerequisites, listed in Prerequisites, are satisfied. In addition, see Important Notes Before You Begin.
2. 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.
3. On the Welcome screen, select the **Create a new WebLogic domain** option. Click **Next**. The Select Domain Source screen is displayed.
4. On the Select Domain Source screen, select the following domain configuration options:

   Oracle Authorization Policy Manager - 11.1.1.3.0 [Oracle_IDM2]

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

   Oracle Identity Manager - 11.1.1.3.0 [Oracle_IDM2]

   Oracle Identity Navigator - 11.1.1.3.0 [Oracle_IDM2]

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

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

6. 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.
7. 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.
8. Choose `JRockit SDK 160_17_R28.0.0-679` 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.
9. On the Configure JDBC Component Schema screen, select a component schema, such as the APM Schema, the SOA Infrastructure Schema, the SOA MDS Schema, the OAM Infrastructure Schema, the OIM MDS Schema, the OIM Schema, the OWSM MDS Schema, the User Messaging Service Schema, or the APM 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.
10. On the Select Optional Configuration screen, you can configure **Administration Server, Managed Servers, Clusters, and Machines**, **Deployments and Services**, **JMS File Store**, and **RDBMS Security 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 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.

      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.
    - Optional: Configure RDBMS Security Store, as required.
11. On the Configuration Summary screen, review the domain configuration, and click **Create** to start creating the domain. After the domain configuration is complete, click **Done** to dismiss the wizard.

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

12. Set up LDAP Synchronization for Oracle Identity Manager, as described in Setting Up LDAP Synchronization.
13. Verify LDAP Synchronization, as described in Verifying the LDAP Synchronization.
14. Start the WebLogic Administration Server and Managed Servers (Oracle Identity Manager and Oracle Access Manager), as described in Starting the Stack.
15. 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=oracle,dc=com",ldapUrl="
       ldap://<oid host>:<oid port>" ,isPrimary="true"
       ,userIDProvider="OracleUserRoleAPI" ,
       groupSearchBase="cn=Groups,dc=us,dc=oracle,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*.

16. 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.
17. On the Welcome screen, select the **Extend an existing WebLogic domain** option. Click **Next**. The Select a WebLogic Domain Directory screen is displayed.
18. On the Select a WebLogic Domain Directory screen, select the Oracle Identity Management domain in which you configured Oracle Identity Manager, Oracle Authorization Policy Manager, Oracle Access Manager, and Oracle Identity Navigator. Click **Next**. The Select Extension Source screen is displayed.
19. On the Select Extension Source screen, select the following domain configuration options:

    Oracle Adaptive Access Manager Admin Server - 11.1.1.3.0 [Oracle_IDM2]
20. After selecting the domain configuration options, click **Next**. The Specify Domain Name and Location screen is displayed.
21. On the Specify Domain Name and Location screen, select a location to store the applications in the domain. Click **Next**. The Configure JDBC Component Schema screen is displayed.
22. On the Configure JDBC Component Schema screen, select a component schema, such as the APM Schema, the OAM Infrastructure Schema, the SOA Infrastructure Schema, the SOA MDS Schema, the OIM MDS Schema, the OIM Schema, the OAAM Admin Schema, the OAAM Admin MDS Schema, the OWSM MDS Schema, the User Messaging Service Schema, or the APM 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.
23. 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.

      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.

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

    Your existing Oracle Identity Management domain with Oracle Identity Manager, Oracle Authorization Policy Manager, Oracle Access Manager, and Oracle Identity Navigator is extended to support Oracle Adaptive Access Manager.

25. Start the Oracle Identity Manager Configuration Wizard, as described in Starting the Oracle Identity Manager 11g Configuration Wizard.

26. 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.

27. Follow the wizard and the steps described in Configuring OIM Server to complete the Oracle Identity ManagerServer 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.

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

15

Configuring Oracle Identity Navigator

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

15.1 General Prerequisites

The following are the general prerequisites for installing and configuring Oracle Identity Management 11*g* Release 1 (11.1.1.3.0) products:

1. Installing Oracle Database, as described in Installing Oracle Database.
2. Installing 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.
3. Installing the Oracle Identity Management 11*g* Release 1 (11.1.1.3.0) suite, as described in Installing OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0). The Oracle Identity Management suite contains Oracle Identity Manager (OIM), Oracle Access Manager (OAM), Oracle Adaptive Access Manager (OAAM), Oracle Authorization Policy Manager (OAPM), and Oracle Identity Navigator (OIN).

15.2 Installing OIN

Oracle Identity Navigator (OIN) is included in the Oracle Identity Management Suite. You can use the Oracle Identity Management 11*g* Installer to install Oracle Identity Management Suite, as described in Installing OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0).

15.3 Important Notes Before You Begin

Before you start installing and configuring Oracle Identity Management products in any of the scenarios discussed in this chapter, keep the following points in mind:

It is assumed that you are installing Oracle Internet Directory, Oracle Virtual Directory, Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Navigator on the same machine.

Note: In this chapter, two IDM_Home directories are mentioned in descriptions and procedures. 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 document. You can specify any name for either of your IDM_Home directories. In addition, you can install the two Oracle Identity Management suites (one containing Oracle Internet Directory, Oracle Virtual Directory, Oracle Directory Services Manager, Oracle Directory Integration Platform, and Oracle Identity Federation; another containing Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Authorization Policy Manager, and Oracle Identity Navigator) 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.

If you have not installed Oracle Internet Directory, Oracle Virtual Directory, Oracle Directory Services Manager, Oracle Directory Integration Platform, or Oracle Identity Federation on the same machine where you are installing Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Authorization Policy Manager, and Oracle Identity Navigator, then you will see a single IDM_Home directory, such as **Oracle_IDM1**, under your MW_HOME directory.

For more information, see Overview and Structure of Oracle Identity Management 11g Installation.

15.4 Configuring Only 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

15.4.1 Appropriate Deployment Environment

Perform the configuration in this topic if you want to configure Oracle Identity Navigator with Oracle Identity Manager, Oracle Access Manager, 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.

15.4.2 Components Deployed

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

15.4.3 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).

15.4.4 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 `<Oracle_IDM2>/common/bin/config.sh` script. (`<Oracle_IDM2>\common\bin\config.cmd` on Windows). The Welcome screen of the Oracle Fusion Middleware Configuration Wizard appears.

   Note: Oracle_IDM2 is used as an example here. You must run this script from your IDM_Home directory that contains Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Authorization Policy Manager, and Oracle Identity Navigator.

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 [Oracle_IDM2]**), and click **Next**. The Specify Domain Name and Location screen appears.

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

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 160_17_R28.0.0-679` 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.

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

15.5 OIN with OIM, OAM, OAAM, and OAPM

This topic describes how to configure Oracle Identity Navigator (OIN) in an existing Oracle Identity Management domain that contains Oracle Identity Manager (OIM), Oracle Access Manager (OAM), Oracle Adaptive Access Manager (OAAM), and Oracle Authorization Policy Manager (OAPM).

It includes the following sections:

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure

15.5.1 Appropriate Deployment Environment

Perform the configuration in this topic if you want to install Oracle Identity Navigator in an existing Oracle Identity Management environment where Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Authorization Policy Manager are installed.

After performing this configuration, you can run the discovery feature of Oracle Identity Navigator to discover the product consoles for Oracle Identity Manager, Oracle Access Manager, and Oracle Adaptive Access Manager. You can view the product consoles in the dashboard of Oracle Identity Navigator. Then you can use the Oracle Identity Navigator user interface to launch consoles for products, such as Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Enterprise Manager Fusion Middleware Control, and so on.

15.5.2 Components Deployed

Performing the configuration in this section deploys the Oracle Identity Navigator application on the existing Administration Server. This application is deployed on the same machine where the Administration Server is running.

15.5.3 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).

15.5.4 Procedure

To configure only Oracle Identity Navigator in an existing Oracle Identity Management domain that contains Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Authorization Policy Manager, 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. 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 `<Oracle_IDM2>/common/bin/config.sh` script. (`<IDM_Home>\common\bin\config.cmd` on Windows). Use the Oracle Fusion Middleware Configuration Wizard to create a new domain to support Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Authorization Policy Manager in the same domain. Ensure that the appropriate domain templates are selected during domain configuration.

   A new domain with the selected configuration is created in the `<MW_HOME>\user_projects\domains` directory (on Windows). On UNIX, the domain is created in the `<MW_HOME>/user_projects/domains` directory.
4. Run the `<Oracle_IDM2>/common/bin/config.sh` script. (`<Oracle_IDM2>\common\bin\config.cmd` on Windows). The Oracle Fusion Middleware Configuration Wizard appears.
5. On the Welcome screen, select the **Extend an existing WebLogic domain** option. Click **Next**.
6. Select your WebLogic domain directory that contains Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Authorization Policy Manager. Click **Next**.
7. On the Select Extension Source screen, ensure that the **Extend my domain automatically to support the following products:** option is selected. Select **Oracle Identity Navigator - 11.1.1.3.0 [Oracle_IDM2]**, and click **Next**. The Configure JDBC Component Schema screen appears.
8. 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.
9. Optional: 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**.
10. 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*.
11. Optional: Assign Managed Servers to clusters, as required.
12. Optional: Configure Machines, as needed. This step is useful when you want to run the Administration Server on one machine and Managed Servers on another physical machine.

    Tip: Before configuring a machine, use the `ping` command to verify whether the machine or host name is accessible.
13. Optional: Assign the Administration Server to a machine.

14. Optional: Select Deployments, such as applications and libraries, and Services to target them to a particular cluster or server.
15. On the Configuration Summary screen, review the domain configuration, and click **Extend** to start extending the domain.

    Your existing Oracle Identity Management domain with Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Authorization Policy Manager is configured to support Oracle Identity Navigator.
16. Start the Oracle Identity Manager Configuration Wizard, as described in Starting the Oracle Identity Manager 11g Configuration Wizard.
17. Configure Oracle Identity Manager Server, as described in Configuring OIM Server.
18. 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.

15.6 Starting the Servers

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

15.7 Verifying OIN

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

8. To exit the Edit mode, click the **Close** button.

   If the task flows are properly added to the page content, the screen displays the task flow content.

9. Test the Product Registration functionality as follows:

   a. Create, edit, or delete the product information by clicking the **Administration** tab.

   b. To add a new product, click the **Create image** icon in the Product Registration section. The New Product Registration dialog pops up.

   c. Enter the relevant information in this dialog, and the new product registration is updated accordingly. The new product registration data is updated on the Launcher portlet after you click the **Dashboard** tab.

   d. Click the product link and ensure that a new browser window or tab opens with the registered product URL.

10. Test the News functionality as follows:

    a. Click the **refresh** icon to update the RSS feed content.

    b. Click the news item link to open the source of content in a new browser window or tab.

11. Test the Reports functionality as follows:

    a. Add a report by clicking the **Add** icon. The Add Report dialog pops up.

    b. In this dialog, select a report to add, and click the **Add Report** button. Verify that the report is added.

    c. Run a report by clicking the report icon. The report opens in a new browser window or tab.

15.8 Getting Started with Oracle OIN After Installation

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

16

Configuring Oracle Identity Manager

This chapter explains how to configure Oracle Identity Manager (OIM) in a new or existing WebLogic domain.

It includes the following topics:

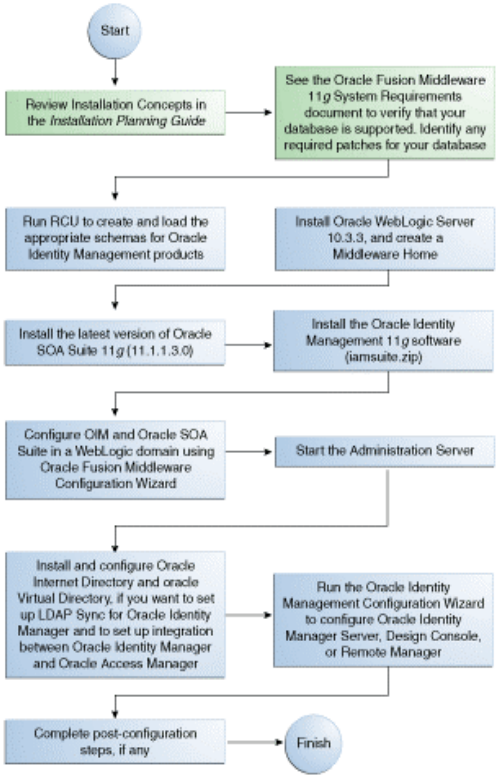
Note: The Oracle Identity Manager Configuration Wizard enables you to configure only some fundamental non-J2EE elements of Oracle Identity Manager, such as Oracle Identity Manager Server, Oracle Identity Manager Design Console, and Oracle Identity Manager Remote Manager. For more information about configuring 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.

16.1 OIM Server Configuration Workflow

The following figure illustrates the process of configuring Oracle Identity Manager (OIM) Server.

Figure 16–1 OIM Server Configuration Workflow



For information about configuring Oracle Identity Manager (OIM) Server on the machine where the Administration Server is running, see Configuring OIM Server.

After configuring OIM Server, you can configure Design Console and Remote Manager on a local or remote machine. For information about configuring OIM Design Console, see Configuring OIM Design Console. For information about configuring Remote Manager, see Configuring OIM Remote Manager.

16.2 Prerequisites

The following are the prerequisites for installing and configuring Oracle Identity Management 11*g* Release 1 (11.1.1.3.0) products:

1. Installing Oracle Database, as described in Installing Oracle Database.
2. Creating and loading schemas using Oracle Fusion Middleware Repository Creation Utility (RCU), as described in Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU).
3. Installing 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.

4. **For Oracle Identity Manager users only**: Installing Oracle SOA Suite 11*g* Release 1 (11.1.1.2.0) and patching it to 11.1.1.3.0, as described in Installing the Latest Version of Oracle SOA Suite (Oracle Identity Manager Users Only).
5. Installing the Oracle Identity Management 11*g* Release 1 (11.1.1.3.0) suite, as described in Installing OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0). The Oracle Identity Management suite contains Oracle Identity Manager (OIM), Oracle Access Manager (OAM), Oracle Adaptive Access Manager (OAAM), Oracle Authorization Policy Manager (OAPM), and Oracle Identity Navigator (OIN).

16.3 Important Notes Before You Start Configuring OIM

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

- It is assumed that you are installing Oracle Internet Directory, Oracle Virtual Directory, Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Navigator on the same machine.

Note: In this chapter, two IDM_Home directories are mentioned in descriptions and procedures. 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 document. You can specify any name for either of your IDM_Home directories. In addition, you can install the two Oracle Identity Management suites (one containing Oracle Internet Directory, Oracle Virtual Directory, Oracle Directory Services Manager, Oracle Directory Integration Platform, and Oracle Identity Federation; another containing Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Authorization Policy Manager, and Oracle Identity Navigator) 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.

If you have not installed Oracle Internet Directory, Oracle Virtual Directory, Oracle Directory Services Manager, Oracle Directory Integration Platform, or Oracle Identity Federation on the same machine where you are installing Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Authorization Policy Manager, and Oracle Identity Navigator, then you will see a single IDM_Home directory, such as **Oracle_IDM1**, under your MW_HOME directory.

For more information, see Overview and Structure of Oracle Identity Management 11g Installation.

- By performing the domain configuration procedures described in this chapter, you can create Managed Servers on a local machine (the machine on which the Administration Server is running). However, you can create and start Managed Servers for Oracle Identity Management components on a remote machine. For more information, see the "Creating and Starting a Managed Server on a Remote Machine" topic in the guide *Oracle Fusion Middleware Creating Templates and Domains Using the Pack and Unpack Commands*.
- You must use the Oracle Identity Manager Configuration Wizard to configure only Oracle Identity Manager Server, Oracle Identity Manager Design Console (on Windows only), and Oracle Identity Manager Remote Manager.

  You must complete this additional configuration for Oracle Identity Manager components after configuring Oracle Identity Manager in a new or existing WebLogic administration domain. For more information, see OIM Domain Configuration Scenarios.

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

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

  Note that Oracle Identity Manager requires Oracle SOA Suite 11*g* (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.

16.4 OIM Domain Configuration Scenarios

The following sections describe basic configuration scenarios for Oracle Identity Manager (OIM):

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

Note: For additional configuration scenarios, see Oracle Identity Management Suite-Level Installation Scenarios.

16.4.1 OIM Without LDAP Sync in a New 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

16.4.1.1 Appropriate Deployment Environment

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

16.4.1.2 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

16.4.1.3 Dependencies

The configuration in this section depends on the following:

- Oracle WebLogic Server.
- Installation of the Oracle Identity Management 11g 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).

16.4.1.4 Procedure

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

1. Ensure that all the prerequisites, listed in Prerequisites, are satisfied. In addition, see Important Notes Before You Start Configuring OIM.
2. Run the `<Oracle_IDM2>/common/bin/config.sh` script (on UNIX). (`<Oracle_IDM2>\common\bin\config.cmd` on Windows). The Welcome screen of the Oracle Fusion Middleware Configuration Wizard appears.
3. On the Welcome screen, select **Create a new WebLogic domain**, and click **Next**. The Select Domain Source screen appears.
4. On the Select Domain Source screen, ensure that the **Generate a domain configured automatically to support the following products:** option is selected.

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

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.

5. Enter a name and a location for the domain to be created, and click **Next**. The Configure Administrator User Name and Password screen appears.
6. Configure a user name and a password for the administrator. The default user name is weblogic. Click **Next**.
7. Choose `JRockit SDK 160_17_R28.0.0-679` 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
8. 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.
9. On the Select Optional Configuration screen, you can configure the **Administration Server**, **JMS Distributed Destination**, **Managed Servers, Clusters, and Machines, Deployments and Services**. Click **Next**.
10. Optional: Configure the following Administration Server parameters:
    - Name
    - Listen address
    - Listen port
    - SSL listen port
    - SSL enabled or disabled

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

    For more information about configuring clusters for Oracle Identity Management products, see the "Configuring High Availability for Identity Management Components" topic in the guide *Oracle Fusion Middleware High Availability Guide*.
14. Optional: Assign Managed Servers to Clusters, as required. Click **Next**.

15. Optional: Configure Machines, as needed. This step is useful when you want to run the Administration Server on one machine and Managed Servers on another physical machine.Click **Next**.

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

16. Optional: Assign servers to machines. Click **Next**.
17. Optional: Select Deployments, such as applications and libraries, and Services to target them to a particular cluster or server. Click **Next**.
18. On the Configuration Summary screen, you can view summaries of your configuration for deployments, application, and service. Review the domain configuration, and click **Create** to start creating the domain.

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

    A new WebLogic domain to support Oracle Identity Manager is created in the `<MW_HOME>\user_projects\domains` directory (on Windows). On UNIX, the domain is created in the `<MW_HOME>/user_projects/domains` directory.
19. Start the Administration Server, as described in Starting or Stopping the Oracle Stack.
20. Start the Oracle Identity Manager Configuration Wizard, as described in Starting the Oracle Identity Manager 11g Configuration Wizard.
21. Configure the Oracle Identity Manager Server, Design Console, or Remote Manager, as described in Configuring OIM Server, Configuring OIM Design Console, and Configuring OIM Remote Manager.

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

16.4.2 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:

- Configuring OIM with LDAP Sync in a New WebLogic Domain
- OIM with LDAP Sync in an Oracle Identity Management 11.1.1.3.0 Domain Containing OID and OVD

16.4.2.1 Configuring OIM with LDAP Sync in a New WebLogic Domain

This section discusses the following topics:

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure

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

16.4.2.1.2 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

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

- Oracle WebLogic Server.
- Installation of the Oracle Identity Management 11g software.
- Installation of the latest version of Oracle SOA Suite.
- Installation of the latest version of Oracle Internet Directory and Oracle Virtual Directory under the same Middleware Home directory or on a different machine.
- 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).

16.4.2.1.4 Procedure Complete the following steps to configure Oracle Identity Manager in a new WebLogic administration domain, to enable LDAP sync, and to configure Oracle Identity Manager Server, Design Console, and Remote Manager:

1. Ensure that all the prerequisites, listed in Prerequisites, are satisfied. In addition, see Important Notes Before You Start Configuring OIM.
2. Run the `<Oracle_IDM2>/common/bin/config.sh` script (on UNIX). (`<Oracle_IDM2>\common\bin\config.cmd` on Windows). The Welcome screen of the Oracle Fusion Middleware Configuration Wizard appears.
3. On the Welcome screen, select **Create a new WebLogic domain**, and click **Next**. The Select Domain Source screen appears.
4. On the Select Domain Source screen, ensure that the **Generate a domain configured automatically to support the following products:** option is selected.

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

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

7. Choose `JRockit SDK 160_17_R28.0.0-679` 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
8. 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.
9. On the Select Optional Configuration screen, you can configure the **Administration Server**, **JMS Distributed Destination**, **Managed Servers, Clusters, and Machines, Deployments and Services**. Click **Next**.
10. Optional: Configure the following Administration Server parameters:
    - Name
    - Listen address
    - Listen port
    - SSL listen port
    - SSL enabled or disabled

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

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

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

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

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

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

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

20. Set up LDAP Synchronization, as described in Setting Up LDAP Synchronization.

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

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

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

16.4.2.2 OIM with LDAP Sync in an Oracle Identity Management 11.1.1.3.0 Domain Containing OID and OVD

This section discusses the following topics:

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure

16.4.2.2.1 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.

16.4.2.2.2 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

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

- Oracle WebLogic Server.
- Installation of the Oracle Identity Management 11g 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).

16.4.2.2.4 Procedure Complete the following steps to configure Oracle Identity Manager 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 11*g* installation is patched to 11.1.1.3.0, as described in Installing OID, OVD, ODSM, ODIP, and OIF (11.1.1.5.0).
3. 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.
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 all the prerequisites, listed in Prerequisites, are satisfied. In addition, see Important Notes Before You Start Configuring OIM.
8. 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.
9. On the Welcome screen, select the **Extend an existing WebLogic domain** option. Click **Next**. The Select a WebLogic Domain Directory screen is displayed.
10. 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.
11. 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]**.

12. After selecting the domain configuration options, click **Next**. The Configure JDBC Component Schema screen is displayed.
13. 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.
14. 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 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.

      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.
15. 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.
16. Start the Administration Server, as described in Starting or Stopping the Oracle Stack.
17. Set up LDAP Synchronization, as described in Setting Up LDAP Synchronization.
18. Verify LDAP Synchronization, as described in Verifying the LDAP Synchronization.
19. Restart the Administration Server, as described in Restarting Servers.
20. Start the Oracle Identity Manager Configuration Wizard, as described in Starting the Oracle Identity Manager 11g Configuration Wizard.
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 BI Publisher 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 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.

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

16.4.3 OIM and OIN in a New WebLogic Domain

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

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure

16.4.3.1 Appropriate Deployment Environment

Perform the configuration in this topic if you want to install Oracle Identity Manager in an environment where you want to use Oracle Identity Navigator as a centralized user interface to discover Oracle Identity Manager. You can also launch the Oracle Identity Administration Console, Oracle Identity Manager Self Service Console, or Oracle Identity Manager Advanced Administration Console from within the Oracle Identity Navigator user interface.

16.4.3.2 Components Deployed

Performing the configuration in this section deploys the following:

- Administration Server
- 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 Managed Server
- Oracle Identity Navigator application on the Administration Server

16.4.3.3 Dependencies

The configuration in this section depends on the following:

- Oracle WebLogic Server.
- Installation of the Oracle Identity Management 11*g* software.
- Installation of the latest version of Oracle SOA Suite.

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

16.4.3.4 Procedure

Perform the following steps to configure Oracle Identity Manager and Oracle Identity Navigator together in a new WebLogic domain:

1. Ensure that all the prerequisites, listed in Prerequisites, are satisfied. In addition, see Important Notes Before You Start Configuring OIM.
2. 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.
3. On the Welcome screen, select the **Create a new WebLogic domain** option. Click **Next**. The Select Domain Source screen is displayed.
4. On the Select Domain Source screen, select the **Generate a domain configured automatically to support the following products:** option.
5. 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 JRF - 11.1.1.0 [oracle_common], **Oracle SOA Suite - 11.1.1.0 [Oracle_SOA1]**, **Oracle WSM Policy Manager - 11.1.1.0 [oracle_common]**, and **Oracle Enterprise Manager - 11.1.1.0 [oracle_common]**

   - **Oracle Identity Navigator - 11.1.1.3.0 [Oracle_IDM2]**
6. After selecting the domain configuration options, click **Next**. The Specify Domain Name and Location screen is displayed.
7. 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.
8. 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.
9. Choose `JRockit SDK 160_17_R28.0.0-679` and Production Mode in the Configure Server Start Mode and JDK screen of the Oracle Fusion Middleware Configuration Wizard. Click **Next**. The JDBC Component Schema screen appears.
10. On the Configure JDBC Component Schema screen, select a component schema, such as the OIM Infrastructure Schema, the SOA Infrastructure Schema, the User Messaging Service Schema, the OWSM MDS Schema, the OIM MDS 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.

11. On the Select Optional Configuration screen, you can configure **Administration Server, Managed Servers, Clusters, and Machines**, **Deployments and Services**, **JMS File Store**, and **RDBMS Security 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 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.

      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.
    - Optional: Configure RDBMS Security Store, as required.
12. On the Configuration Summary screen, review the domain configuration, and click **Create** to start creating the domain. After the domain configuration is complete, click **Done**.

    A new WebLogic domain to support Oracle Identity 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.

    Note: If you want to start the SOA Server on a remote machine, then you must manually copy the composite files from the `<DOMAIN_HOME>/soa/autodeploy` directory on the local machine to the `<DOMAIN_HOME>/soa/autodeploy` directory on the remote machine after running the `unpack` command on the remote machine. If the `<DOMAIN_HOME>/soa/autodeploy` directory does not exist on the remote machine, you must create this directory before copying the composite files.
13. Start the Oracle Identity Manager Configuration Wizard, as described in Starting the Oracle Identity Manager 11g Configuration Wizard.

14. Configure Oracle Identity Manager Server, as described in Configuring OIM Server.
15. 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.

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

16.4.4 OIM and OAM in a WebLogic Domain Containing OIN

This topic describes how to configure Oracle Identity Manager (OIN) and Oracle Access Manager (OAM) together in a WebLogic administration domain that has Oracle Identity Navigator (OIN) installed. It includes the following sections:

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure

16.4.4.1 Appropriate Deployment Environment

Perform the configuration in this topic if you want to install Oracle Identity Manager and Oracle Access Manager in an environment where Oracle Identity Navigator is already installed. You can set up integration between Oracle Identity Manager and Oracle Access Manager, as described in Integration Between OIM and OAM. You can use the Oracle Identity Navigator user interface to discover and access product consoles for Oracle Identity Manager and Oracle Access Manager.

16.4.4.2 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 Administration Server

16.4.4.3 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 (this is 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).
- Configuration of Oracle Identity Navigator in a new WebLogic domain.

16.4.4.4 Procedure

Perform the following steps to configure Oracle Identity Manager and Oracle Access Manager in a WebLogic domain that has Oracle Identity Navigator installed:

1. Ensure that all the prerequisites, listed in Prerequisites, are satisfied. In addition, see Important Notes Before You Start Configuring OIM.
2. Configure only Oracle Identity Navigator in a new WebLogic domain, as described in Configuring Only OIN in a New WebLogic Domain.
3. Verify the installation of Oracle Identity Navigator, as described in Verifying OIN.
4. 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.
5. 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.
6. On the Welcome screen, select the **Extend an existing WebLogic domain** option. Click **Next**.
7. On the Select a WebLogic Domain Directory screen, browse to the directory that contains the WebLogic domain in which you configured Oracle Identity Navigator. Click **Next**. The Select Extension Source screen appears.
8. 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]**, **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]**
9. After selecting the domain configuration options, click **Next**. The Specify Domain Name and Location screen is displayed.
10. On the Specify Domain Name and Location screen, enter a location to store applications for the domain. Click **Next**. The Configure JDBC Component Schema screen is displayed.
11. On the Configure JDBC Component Schema screen, select a component schema, such as the OIM Infrastructure Schema, the SOA Infrastructure Schema, the User Messaging Service Schema, the OWSM MDS Schema, the OIM MDS 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.

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.

      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.
13. On the Configuration Summary screen, review the domain configuration, and click **Extend** to start extending the domain. When the domain configuration is complete, click **Done**.

    The existing Oracle Identity Navigator domain is configured to support Oracle Identity Manager and Oracle Access Manager.

    Note: If you want to start the SOA Server on a remote machine, then you must manually copy the composite files from the `<DOMAIN_HOME>/soa/autodeploy` directory on the local machine to the `<DOMAIN_HOME>/soa/autodeploy` directory on the remote machine after running the `unpack` command on the remote machine. If the `<DOMAIN_HOME>/soa/autodeploy` directory does not exist on the remote machine, you must create this directory before copying the composite files.

    ---
14. Restart the Administration Server, as described in Restarting Servers.
15. Start the Oracle Identity Manager Configuration Wizard, as described in Starting the Oracle Identity Manager 11g Configuration Wizard.
16. Configure Oracle Identity Manager Server, as described in Configuring OIM Server.
17. 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.

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

16.4.5 OIM and OIN in a WebLogic Domain Containing OAM

This topic describes how to configure Oracle Identity Manager (OIM) and Oracle Identity Navigator (OIN) together in a WebLogic domain that has Oracle Access Manager (OAM) installed. It includes the following sections:

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure

16.4.5.1 Appropriate Deployment Environment

Perform the configuration in this topic if you want to install Oracle Identity Manager and Oracle Identity Navigator in an Oracle Identity Management environment where Oracle Access Manager is already installed. You can set up integration between Oracle Identity Manager and Oracle Access Manager, as described in Integration Between OIM and OAM. You can use the Oracle Identity Navigator user interface to discover and access product consoles for both Oracle Identity Manager and Oracle Access Manager.

16.4.5.2 Components Deployed

Performing the configuration in this section deploys the following:

- 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
- Oracle Identity Navigator application on the existing Administration Server

16.4.5.3 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, Oracle SOA Suite, and Oracle Access Manager. For more information, see Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU).
- Configuration of Oracle Access Manager in a new WebLogic domain.

16.4.5.4 Procedure

Perform the following steps to configure Oracle Identity Manager and Oracle Identity Navigator together in a WebLogic administration domain that has Oracle Access Manager installed:

1. Ensure that all the prerequisites, listed in Prerequisites, are satisfied. In addition, see Important Notes Before You Start Configuring OIM.
2. Configure only Oracle Access Manager in a new WebLogic domain, as described in OAM in a New WebLogic Domain.
3. Verify the installation of Oracle Access Manager, as described in Verifying the OAM Installation.
4. 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.
5. On the Welcome screen, select the **Extend an existing WebLogic domain** option. Click **Next**.
6. On the Select a WebLogic Domain Directory screen, browse to the directory that contains the WebLogic domain in which you configured Oracle Access Manager. Click **Next**. The Select Extension Source screen appears.
7. 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]**, **Oracle Enterprise Manager - 11.1.1.0 [oracle_common]**, and **Oracle WSM Policy Manager - 11.1.1.0 [oracle_common]**.

   - **Oracle Identity Navigator - 11.1.1.3.0 [Oracle_IDM2]**
8. After selecting the domain configuration options, click **Next**. The Specify Domain Name and Location screen is displayed.
9. On the Specify Domain Name and Location screen, enter a location to store applications for the domain. 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 OIM Infrastructure Schema, the SOA Infrastructure Schema, the User Messaging Service Schema, the OWSM MDS Schema, the OIM MDS 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.
11. 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.

  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.

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

    Your existing WebLogic domain with Oracle Access Manager is extended to support Oracle Identity Manager and Oracle Identity Navigator.

    Note: If you want to start the SOA Server on a remote machine, then you must manually copy the composite files from the `<DOMAIN_HOME>/soa/autodeploy` directory on the local machine to the `<DOMAIN_HOME>/soa/autodeploy` directory on the remote machine after running the `unpack` command on the remote machine. If the `<DOMAIN_HOME>/soa/autodeploy` directory does not exist on the remote machine, you must create this directory before copying the composite files.

13. Restart the Administration Server, as described in Restarting Servers.
14. Start the Oracle Identity Manager Configuration Wizard, as described in Starting the Oracle Identity Manager 11g Configuration Wizard.
15. Configure Oracle Identity Manager Server, as described in Configuring OIM Server.
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.

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

16.4.6 OIM, OAM, and OIN in a New WebLogic Domain

This topic describes how to configure Oracle Identity Manager (OIM), Oracle Access Manager (OAM), and Oracle Identity Navigator (OIN) together in a new WebLogic administration domain. It includes the following sections:

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure

16.4.6.1 Appropriate Deployment Environment

Perform the configuration in this topic if you want to install Oracle Identity Manager, Oracle Access Manager, and Oracle Identity Navigator together in an Oracle Identity Management environment. You can set up integration between Oracle Identity Manager and Oracle Access Manager, as described in Integration Between OIM and OAM. You can use the Oracle Identity Navigator user interface to discover and access product consoles for Oracle Identity Manager and Oracle Access Manager.

At a later time, you can also add Oracle Adaptive Access Manager to this environment and set up integration between Oracle Access Manager and Oracle Adaptive Access Manager.

16.4.6.2 Components Deployed

Performing the configuration in this section deploys the following:

- 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 Identity Navigator application and Oracle Access Manager Console on the Administration Server

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

16.4.6.4 Procedure

Perform the following steps to configure Oracle Identity Manager, Oracle Access Manager, and Oracle Identity Navigator together in a new WebLogic domain:

1. Ensure that all the prerequisites, listed in Prerequisites, are satisfied. In addition, see Important Notes Before You Start Configuring OIM.

2. 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.
3. On the Welcome screen, select the **Create a new WebLogic domain** option. Click **Next**. The Select Domain Source screen is displayed.
4. On the Select Domain Source screen, select the **Generate a domain configured automatically to support the following products:** option.
5. 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]**, **Oracle JRF - 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]**
   - **Oracle Identity Navigator - 11.1.1.3.0 [Oracle_IDM2]**
6. After selecting the domain configuration options, click **Next**. The Specify Domain Name and Location screen is displayed.
7. 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.
8. 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.
9. Choose `JRockit SDK 160_17_R28.0.0-679` and Production Mode in the Configure Server Start Mode and JDK screen of the Oracle Fusion Middleware Configuration Wizard. Click **Next**. If you selected **Oracle Access Manager with Database Policy Store - 11.1.1.3.0 [Oracle_IDM2]** option on the Select Extension Source screen, the Configure JDBC Data Sources Screen is displayed. Configure the `oamDS` data source, as required. After the test succeeds, the Configure JDBC Component Schema screen is displayed.
10. On the Configure JDBC Component Schema screen, select a component schema, such as the OIM Infrastructure Schema, the SOA Infrastructure Schema, the User Messaging Service Schema, the OWSM MDS Schema, the OIM MDS 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.
11. On the Select Optional Configuration screen, you can configure **Administration Server, Managed Servers, Clusters, and Machines**, **Deployments and Services**, **JMS File Store**, and **RDBMS Security 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 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.

  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.
- Optional: Configure RDBMS Security Store, 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 Identity Manager, Oracle 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.

    Note: If you want to start the SOA Server on a remote machine, then you must manually copy the composite files from the `<DOMAIN_HOME>/soa/autodeploy` directory on the local machine to the `<DOMAIN_HOME>/soa/autodeploy` directory on the remote machine after running the `unpack` command on the remote machine. If the `<DOMAIN_HOME>/soa/autodeploy` directory does not exist on the remote machine, you must create this directory before copying the composite files.
13. Start the Oracle Identity Manager Configuration Wizard, as described in Starting the Oracle Identity Manager 11g Configuration Wizard.
14. Configure Oracle Identity Manager Server, as described in Configuring OIM Server.
15. 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.

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

16.5 Starting the Servers

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

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

16.6 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.

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

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

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

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.

This section discusses the following topics:

- Scope of Configuration Using the Oracle Identity Manager 11g Configuration Wizard
- Scenario 1: Oracle Identity Manager Server and Design Console on Different Machines

- Scenario 2: Oracle Identity Manager Server and Remote Manager on Different Machines
- Scenario 3: Oracle Identity Manager Server, Design Console, and Remote Manager on a Single Windows Machine

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

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

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

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

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

1. Install and configure Oracle Identity Manager Server on a machine after completing all the prerequisites, as described in Configuring OIM Server. Ensure that the Oracle Identity Manager Server is up and running.
2. On a different Windows machine, 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).
3. On the Windows machine where you installed the Oracle Identity Management 11*g* (11.1.1.3.0) software, run the Oracle Identity Manager Configuration Wizard to configure only Design Console. Note that you must provide the Oracle Identity Manager Server information, such as host and URL, when configuring Design Console. For more information, see Installing and Configuring Only OIM Design Console on Windows.

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

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

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

1. Install and configure Oracle Identity Manager Server on a machine after completing all the prerequisites, as described in Configuring OIM Server. Ensure that the Oracle Identity Manager Server is up and running.
2. On a different machine, 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).

3. On the machine where you installed the Oracle Identity Management 11*g* (11.1.1.3.0) software, run the Oracle Identity Manager Configuration Wizard to configure only Remote Manager. Note that you must provide the Oracle Identity Manager Server information, such as host and URL, when configuring Remote Manager. For more information, see Configuring OIM Remote Manager.

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

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

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

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

16.7 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

16.7.1 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 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).
5. 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).
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 following example scenarios:
   - OIM Without LDAP Sync in a New Domain
   - OIM with LDAP Sync
   - OIM and OIN in a New WebLogic Domain
   - OIM and OAM in a WebLogic Domain Containing OIN
   - OIM and OIN in a WebLogic Domain Containing OAM
   - OIM, OAM, and OIN in a New WebLogic Domain
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: Installing Oracle HTTP Server 11*g* Webgate for Oracle Access Manager, if you want to set up integration between Oracle Identity Manager and Oracle Access Manager. For more information, see Migrating from Domain Agent to Oracle HTTP Server 10g Webgate for OAM.
9. Optional: Setting up LDAP Synchronization for Oracle Identity Manager, if you want to enable LDAP Sync. For more information, see Setting Up LDAP Synchronization.
10. 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*.

16.7.2 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 remote machine. In addition, the Oracle Identity Manager Server should be up and running.

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

16.7.3 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.

16.8 Starting the Oracle Identity Manager 11*g* Configuration Wizard

To start the Oracle Identity Manager 11*g* Configuration Wizard, execute the `<Oracle_IDM2>/bin/config.sh` script (on UNIX) on the machine where the Administration Server is running. (`<Oracle_IDM2>\bin\config.bat` on Windows). The Oracle Identity Management 11*g* Configuration Wizard starts, and the Welcome Screen appears.

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

16.9 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

16.9.1 Appropriate Deployment Environment

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

16.9.2 Components Deployed

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

16.9.3 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 Preparing to Install Oracle Identity Management and Installing OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0).

16.9.4 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. In addition, see Important Notes Before You Start Configuring OIM.
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 Setting Up LDAP Synchronization, 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. This password is generated when you run the configureOIM WLST command to configure Oracle Access Manager (OAM) for Oracle Identity Manager (OIM) integration. For more information about this WLST command and the complete setup to integrate OIM and OAM, see Setting Up Integration Between OIM and OAM Using the Domain Agent.
    - **Domain of Cookie** - Enter the domain of the machine on which Oracle HTTP Server for Oracle Identity Manager is running. For example, examplehost.exampledomain.com

    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=oracle, dc=com. SearchDN is the OVD searchbase 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. For more information, see Verifying the LDAP Synchronization. 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 Performing a Silent Installation.

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

    A configuration log is saved to the `logs` directory under Oracle Inventory directory. For information about the log files, see 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.

16.9.5 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 apply the Patch 9819201 as follows:

  1. Go to My Oracle Support at `http://support.oracle.com`, click on the **Patches & Updates** tab, and search for patch 9819201.
  2. Download the patch and install it by following the instructions in the README file included with the patch.

16.10 Installing and Configuring Only OIM Design Console on Windows

Table 16–1 lists the steps required to install and configure only Oracle Identity Manager (OIM) Design Console on Windows operating systems.

Table 16–1 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 and Scenario 1: Oracle Identity Manager Server and Design Console on Different Machines.

16.11 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
- Updating the xlconfig.xml File to Change the Port for Design Console
- Configuring Design Console to Use SSL

16.11.1 Appropriate Deployment Environment

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

16.11.2 Components Deployed

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

16.11.3 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.

16.11.4 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. In addition, see Important Notes Before You Start Configuring OIM.
2. On the Windows machine where Oracle Identity Manager Design Console sound 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 Performing a Silent Installation.

   After you click **Configure**, the Configuration Progress screen appears. A configuration log is saved to the `logs` directory under Oracle Inventory directory. For information about the log files, see 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.

16.11.5 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.

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

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

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

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

16.11.7 Configuring Design Console to Use SSL

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

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

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

b. Edit the <ApplicationURL> entry to use HTTPS, T3S protocol, and SSL port to connect to the server, as in the following example:

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

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

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

---

c. Save the file and exit.

16.12 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

16.12.1 Appropriate Deployment Environment

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

16.12.2 Components Deployed

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

16.12.3 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.

16.12.4 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. In addition, see Important Notes Before You Start Configuring OIM.
2. On the machine where Oracle Identity Manager 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 Performing a Silent Installation.

   ---

9. After you click **Configure**, the Configuration Progress screen appears. A configuration log is saved to the `logs` directory under Oracle Inventory directory. For information about the log files, see 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.

16.13 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`.

16.14 Setting Up LDAP Synchronization

This section discusses the following topics:

1. Prerequisites
2. Task 1: Running the LDAP Preconfiguration Utility
3. Task 2: Configuring OVD and OID for OIM
4. Task 3: Running the LDAP Post-Configuration Utility
5. After Setting Up LDAP Synchronization
6. Verifying the LDAP Synchronization

16.14.1 Prerequisites

You must complete the following prerequisites for setting up LDAP synchronization:

1. Install a supported version of Oracle Database, as described in Installing Oracle Database.
2. Create and load database schemas, as described in Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU).
3. Ensure that the Oracle Identity Management 11*g* Release 1 (11.1.1.3.0) suite containing Oracle Internet Directory (OID) and Oracle Virtual Directory (OVD) are installed, as described in Installing OID, OVD, ODSM, ODIP, and OIF (11.1.1.5.0).
4. Configure Oracle Internet Directory (OID) and Oracle Virtual Directory (OVD) with or without a WebLogic administration domain. For more information, see Configuring Oracle Internet Directory and Configuring Oracle Virtual Directory.
5. Install Oracle Identity Management 11*g* Release 1 (11.1.1.3.0) suite containing Oracle Identity Manager (OIM), Oracle Access Manager (OAM), Oracle Adaptive Access Manager (OAAM), 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).

16.14.2 Task 1: Running the LDAP Preconfiguration Utility

After completing the prerequisites, you must run the LDAP preconfiguration utility as follows:

1. Open the `ldapconfig.props` file in a text editor. This file is located in the `server/ldap_config_util` directory under the Oracle Home for Oracle Identity Manager and Oracle Acccess Manager.
2. In the `ldapconfig.props` file, set values for the following parameters:

- **OIMProviderURL** - Specify the URL for the OIM provider in the format: `t3://localhost:port`. For example:

  ```
  t3://myhost.mycompany.com:8003
  ```

- **OIDURL** - Specify the URL for the OID instance.
- **OIDAdminUsername** - Specify the OID Administrator's user name, such as `cn=orcladmin`.
- **OIDSearchBase** - Specify the OID search base, such as `ou=people,dc=com`.
- **UserContainerName** - Specify the name of the user container, which is used as a default container of users in the LDAP directory.
- **RoleContainerName** - Specify the name of the role container, which is used as a default container of roles in the LDAP directory.
- **ReservationContainerName** - Specify the name of the user reservation container, which is used to reserve users while waiting for user creation approvals in Oracle Identity Manager. When the user creation is approved, users are moved from the reservation container to the actual user container.

3. Ensure that the *WL_HOME* environment variable is set to the `wlserver_10.3` directory under your Middleware Home. On UNIX, it is the `<MW_HOME>/wlserver_10.3` directory. On Windows, it is the `<MW_HOME>\wlserver_10.3` directory. In addition, set the *JAVA_HOME* environment variable to the directory where the JDK is installed on your machine.
4. On the command line, run the LDAP configuration pre-setup script (`LDAPConfigPreSetup.bat` on Windows, and `LDAPConfigPreSetup.sh` on UNIX). The files are located in the same `server/ldap_config_util` directory under your IDM_Home for Oracle Identity Manager and Oracle Access Manager.
5. When prompted, enter the OID administrator's password and the OIM administrator's password.

16.14.3 Task 2: Configuring OVD and OID for OIM

After running the LDAP preconfiguration utility, as described in Task 1: Running the LDAP Preconfiguration Utility, you must create and configure two Oracle Virtual Directory (OVD) adapters and Changelog adapters.

To configure the adapters, complete the following steps:

1. Create a User adapter as follows:
   a. Choose the **User_OID** template.
   b. Specify **Proxy DN** as follows: `cn=oimadmin,cn=users,cn=oim,cn=products,cn=oraclecontext`
   c. Specify **Proxy Password** as the value that is specified for the `oimadmin` user.
   d. For **namespace**, select **Remote Base** and map it to **Mapped Namespace** in Oracle Virtual Directory.
2. Create a Changelog adapter as follows:
   a. Choose the **Changelog_OID** template.
   b. For **namespace**, set both **Remote Base** and map it to **Mapped Namespace** to `cn=changelog`.

3. Verify that the plug-in parameter values for the user adapter match with the values listed in Table 16–2.
   a. Select the user adapter to modify, and click the **Plug-ins** tab.
   b. Click the plug-in, and click **Edit**.
   c. In the Parameters table, update the parameters, if necessary, to match the following values:

Table 16–2 User Adapter Parameter Values

Parameter	Value
directoryType	oid
pwdMaxFailure	10
oamEnabled	true or false Note that this parameter should be set to true if you are setting up integration between Oracle Identity Manager and Oracle Access Manager.

   d. Click **OK**.
   e. Click **Apply**.
4. Verify that the plug-in parameter values for the changelog adapter match with the values listed in Table 16–3.
   a. Select the changelog adapter to modify, and click the **Plug-ins** tab.
   b. Click the plug-in, and click **Edit**.
   c. In the Parameters table, update the parameters, if necessary, to match the following values:

Table 16–3 Changelog Adapter Parameter Values

Parameter	Value
directoryType	oid
mapAttribute	targetGUID=orclGUID
mapObjectclass	changelog=changelogentry
requiredAttribute	orclGUID
addAttribute	orclContainerOC,changelogSupported=1
modifierDNFilter	cn=oimadmin,cn=users,cn=OIM,cn=Products,cn=OracleContext
sizeLimit	1000
targetDNFilter	Search based from which reconciliation needs to happen. This value needs to same as the LDAP SearchDN that is specified during OIM installation
mapUserState	true
oamEnabled	true or false

   d. Click **OK**.
   e. Click **Apply**.

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

16.14.4 Task 3: Running the LDAP Post-Configuration Utility

After configuring OID and OVD for OIM, as described in Task 2: Configuring OVD and OID for OIM, you must run the LDAP post-configuration utility as follows:

1. In the `ldapconfig.props` file, set values for the following parameters:
   - **OIMProviderURL** - Specify the URL for the OIM provider in the format: `t3://localhost:8003`
   - **OIDURL** - Specify the URL for the OID instance.
   - **OIDAdminUsername** - Specify the OID Administrator's user name, such as `cn=orcladmin`.
   - **OIDSearchBase** - Specify the OID search base, such as `ou=people,dc=com`.
   - **UserContainerName** - Specify the name of the user container, which is used as a default container of users in the LDAP directory.
   - **RoleContainerName** - Specify the name of the user container, which is used as a default container of roles in the LDAP directory.
   - **ReservationContainerName** - Specify the name of the user reservation container, which is used to reserve users while waiting for user creation approvals in Oracle Identity Manager. When the user creation is approved, users are moved from the reservation container to the actual user container.
2. Ensure that the *WL_HOME* environment variable is set to the `wlserver_10.3` directory under your Middleware Home. On UNIX, it is the `<MW_HOME>/wlserver_10.3` directory. On Windows, it is the `<MW_HOME>\wlserver_10.3` directory. In addition, set the *JAVA_HOME* environment variable to the directory where the JDK is installed on your machine.
3. Start the OIM Managed Server. For more information, see Starting the Servers.
4. On the command line, run the LDAP configuration post-setup script (`LDAPConfigPostSetup.bat` on Windows, and `LDAPConfigPostSetup.sh` on UNIX). The files are located in the `server/ldap_config_util` directory under your IDM_Home for Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Authorization Policy Manager, and Oracle Identity Navigator.
5. When prompted, enter the OIM administrator's password and the `xelsysadm` password.

16.14.5 After Setting Up LDAP Synchronization

After setting up LDAP synchronization, you can enable LDAP Sync for Oracle Identity Manager by selecting the **Enable LDAP Sync** option on the BI Publisher and OAM screen in the Oracle Identity Management 11*g* Configuration Wizard while configuring Oracle Identity Manager (OIM) Server. For more information, see Configuring OIM Server.

Note that LDAP Sync is enabled automatically if you choose to enable identity administration integration with Oracle Access Manager on the BI Publisher and OAM screen.

16.14.6 Verifying the LDAP Synchronization

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

1. Ensure that the WebLogic Administration Server is up and running.
2. Invoke the Oracle Identity Manager Administration Console (`http://<host>:<port>/oim`), which is deployed on the Administration Server.
3. In this console, click **Search** under **Configurations** -> **Manage IT Resource**. If the LDAP information is correct, the resource information is displayed.
4. Create a normal user using the same console.
5. If a user is created, verify the LDAP store by using the Oracle Data Services Manager URL, such as `http://<host>:<odsm_port>/odsm/faces/odsm.jspx`.

Note: Ensure that Oracle Identity Directory being used has an Oracle Virtual Directory configured. They both must be up and running because Oracle Identity Manager communicates with the LDAP data store via the Oracle Virtual Directory component.

16.15 Setting Up Integration with OAM

For information about setting up integration between Oracle Identity Manager (OIM) and Oracle Access Manager (OAM), see Integration Between OIM and OAM.

16.16 List of Supported Languages

Oracle Identity Manager supports the following languages:

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

16.17 Using the Diagnostic Dashboard

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

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

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

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

16.18 Getting Started with OIM After Installation

After installing Oracle Identity Manager (OIM), refer to "Part 1: Oracle Identity Manager System Administration Console" and "Part 2: Oracle Identity Manager Administrative and User Console" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.

17

Configuring Oracle Access Manager

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

17.1 Prerequisites

The following are the prerequisites for installing and configuring Oracle Identity Management 11*g* Release 1 (11.1.1) products:

1. Installing Oracle Database, as described in Installing Oracle Database.
2. Installing 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.
3. Creating and loading schemas using Oracle Fusion Middleware Repository Creation Utility (RCU), as described in Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU).
4. Installing the Oracle Identity Management 11*g* Release 1 (11.1.1.3.0) suite, as described in Installing OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0). The Oracle Identity Management suite contains Oracle Identity Manager (OIM), Oracle

Access Manager (OAM), Oracle Adaptive Access Manager (OAAM), Oracle Authorization Policy Manager (OAPM), and Oracle Identity Navigator (OIN).

17.2 Important Notes Before You Begin

Before you start installing and configuring Oracle Identity Management products in any of the scenarios discussed in this chapter, keep the following points in mind:

It is assumed that you are installing Oracle Internet Directory, Oracle Virtual Directory, Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Navigator on the same machine.

Note: In this chapter, two IDM_Home directories are mentioned in descriptions and procedures. 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 document. You can specify any name for either of your IDM_Home directories. In addition, you can install the two Oracle Identity Management suites (one containing Oracle Internet Directory, Oracle Virtual Directory, Oracle Directory Services Manager, Oracle Directory Integration Platform, and Oracle Identity Federation; another containing Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Authorization Policy Manager, and Oracle Identity Navigator) 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.

If you have not installed Oracle Internet Directory, Oracle Virtual Directory, Oracle Directory Services Manager, Oracle Directory Integration Platform, or Oracle Identity Federation on the same machine where you are installing Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Authorization Policy Manager, and Oracle Identity Navigator, then you will see a single IDM_Home directory, such as **Oracle_IDM1**, under your MW_HOME directory.

For more information, see Overview and Structure of Oracle Identity Management 11g Installation.

17.3 Installing OAM

Oracle Access Manager (OAM) is included in the Oracle Identity Management Suite. You can use the Oracle Identity Management 11*g* Installer to install the Oracle Identity Management Suite. For more information, see Preparing to Install Oracle Identity Management and Installing OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0).

17.4 Oracle Access Manager Domain Configuration Template

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

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

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

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

For a list of screens in the Oracle Fusion Middleware Configuration Wizard, see Screens in Oracle Fusion Middleware Configuration Wizard.

17.5 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:

17.5.1 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 11*g* components, such as Oracle Identity Navigator, Oracle Identity Manager, and Oracle Adaptive Access Manager at a later time in the same domain.

17.5.2 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

17.5.3 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. For more information, see Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU).

17.5.4 Procedure

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

1. Ensure that all prerequisites, listed in Prerequisites, are satisfied. In addition, see Important Notes Before You Begin.
2. 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.
3. On the Welcome screen, select the **Create a new WebLogic domain** option. Click **Next**. The Select Domain Source screen appears.
4. On the Select Domain Source screen, ensure that the **Generate a domain configured automatically to support the following products:** option is selected. Select **Oracle Access Manager with Database Policy Store - 11.1.1.3.0 [Oracle_IDM2]**, and click **Next**. The Select Domain Name and Location screen appears.

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

5. Enter a name and a location for the domain to be created, and click **Next**. The Configure Administrator User Name and Password screen appears.
6. Configure a user name and a password for the administrator. The default user name is `weblogic`. Click **Next**.
7. Choose `JRockit SDK 160_17_R28.0.0-679` 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.
8. On the Configure JDBC Component Schema screen, select a component schema, such as the OAM Infrastructure Schema that you want to modify.

   You can set values for Schema Owner, Schema Password, Database and Service, Host Name, and Port. Click **Next**. The Test JDBC Component Schema screen appears. After the test succeeds, the Select Optional Configuration screen appears.
9. On the Select Optional Configuration screen, you can configure the **Administration Server** and **Managed Servers, Clusters, and Machines**. 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.

    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.

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.

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

15. 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.

16. Optional: Assign the newly created Managed Server, such as `oam_server1`, to a machine.

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

A new WebLogic domain to support Oracle 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.

17.6 OAM and OIN in a New WebLogic Domain

This topic describes how to configure Oracle Access Manager (OAM) and Oracle Identity Navigator (OIN) together in a new WebLogic domain. It includes the following sections:

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure

17.6.1 Appropriate Deployment Environment

Perform the configuration in this topic if you want to install Oracle Access Manager in an environment where you may add other Oracle Identity Management products, such as Oracle Identity Access Manager and Oracle Adaptive Access Manager, at a later time. You can use Oracle Identity Navigator to discover and launch the Oracle Access Manager Console from within the Oracle Identity Navigator user interface.

17.6.2 Components Deployed

Performing the configuration in this section deploys the following:

- Administration Server
- Managed Server for Oracle Access Manager
- Oracle Access Manager Console and Oracle Identity Navigator application on the Administration Server

17.6.3 Dependencies

The configuration in this section depends on the following:

- Oracle WebLogic Server.
- Installation of the Oracle Identity Management 11*g* software.
- Database schemas for Oracle Access Manager. For more information, see Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU).

17.6.4 Procedure

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

1. Ensure that all prerequisites, listed in Prerequisites, are satisfied. In addition, see Important Notes Before You Begin.
2. 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.
3. On the Welcome screen, select the **Create a new WebLogic domain** option. Click **Next**. The Select Domain Source screen is displayed.
4. On the Select Domain Source screen, select the **Generate a domain configured automatically to support the following products:** option.
5. Select the following domain configuration options:
   - **Oracle Access Manager with Database Policy Store - 11.1.1.3.0 [Oracle_IDM2]**

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

   - **Oracle Identity Navigator - 11.1.1.3.0 [Oracle_IDM2]**
6. After selecting the domain configuration options, click **Next**. The Specify Domain Name and Location screen is displayed.
7. 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.

8. 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.
9. Choose `JRockit SDK 160_17_R28.0.0-679` and **Production Mode** in the Configure Server Start Mode and JDK screen of the Oracle Fusion Middleware Configuration Wizard. Click **Next**. The Configure JDBC Data Sources Screen is displayed.
10. On the Configure JDBC Sources screen, configure the `oamDS` data source, as required. After the test succeeds, the Select Optional Configuration screen is displayed.
11. On the Select Optional Configuration screen, you can configure **Administration Server, Managed Servers, Clusters, and Machines**, **Deployments and Services**, and **RDBMS Security 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 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.

      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.
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 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.

17.7 OAM in a Domain Containing OIM and OIN

This topic describes how to configure Oracle Access Manager (OAM) in a Oracle Identity Management domain that has Oracle Identity Manager (OIM) and Oracle Identity Navigator (OIN) installed. It includes the following sections:

- Appropriate Deployment Environment
- Components Deployed

17.7.1 Appropriate Deployment Environment

Perform the configuration in this topic if you want to install Oracle Access Manager in an environment where Oracle Identity Manager and Oracle Identity Navigator are already installed. You can use Oracle Identity Navigator to discover and launch the Oracle Access Manager Console and the Oracle Identity Manager Consoles (Oracle Identity Administration Console, Oracle Identity Manager Self Service Console, and Oracle Identity Manager Advanced Administration Console) from within the Oracle Identity Navigator user interface. At a later time, you can also set up integration between Oracle Identity Manager and Oracle Access Manager, as described in Integration Between OIM and OAM.

17.7.2 Components Deployed

Performing the configuration in this section deploys the following:

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

17.7.3 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, Oracle SOA Suite, and Oracle Access Manager. For more information, see Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU).
- Installation and configuration of Oracle Identity Manager with Oracle Identity Navigator in a new WebLogic domain.

17.7.4 Procedure

Perform the following steps to configure Oracle Access Manager in a WebLogic domain that contains Oracle Identity Manager and Oracle Identity Navigator:

1. Ensure that all prerequisites, listed in Prerequisites, are satisfied. In addition, see Important Notes Before You Begin.
2. Configure Oracle Identity Manager and Oracle Identity Navigator in a new WebLogic domain, as described in OIM and OIN in a New WebLogic Domain. A new WebLogic domain to support Oracle Identity 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.
3. 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.

4. On the Welcome screen, select the **Extend an existing WebLogic domain** option. Click **Next**.
5. On the Select a WebLogic Domain Directory screen, browse to the directory that contains the WebLogic domain in which you configured Oracle Identity Manager and Oracle Identity Navigator. Click **Next**. The Select Extension Source screen appears.
6. On the Select Extension Source screen, select the **Oracle Access Manager with Database Policy Store - 11.1.1.3.0 [Oracle_IDM2]** domain configuration option.
7. After selecting the domain configuration options, click **Next**. The Configure JDBC Data Sources Screen is displayed. Configure the `oamDS` data source, as required. After the test succeeds, the Configure JDBC Component Schema screen is displayed.
8. On the Configure JDBC Component Schema screen, select a component schema, such as the OIM Infrastructure Schema, the SOA Infrastructure Schema, the User Messaging Service Schema, the OWSM MDS Schema, the OIM MDS 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 **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.

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

    Your existing WebLogic domain with Oracle Identity Manager and Oracle Identity Navigator is extended to support Oracle Access Manager.

17.8 OAM in a Domain Containing OAAM and OIN

This topic describes how to configure Oracle Access Manager (OAM) in an Oracle Identity Management domain that has Oracle Adaptive Access Manager (OAAM) and Oracle Identity Navigator (OIN) installed. It includes the following sections:

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure

17.8.1 Appropriate Deployment Environment

Perform the configuration in this topic if you want to install Oracle Access Manager in an environment where Oracle Adaptive Access Manager and Oracle Identity Navigator are already installed. At a later time, you may install Oracle Identity Manager in the same domain and set up integration between Oracle Access Manager and Oracle Identity Manager. You can also set up integration between Oracle Adaptive Access Manager and Oracle Access Manager, as described in the "Integrating OIM, OAM, and OAAM" topic in the *Oracle Fusion Middleware Developer's Guide for Oracle Adaptive Access Manager*.

You can use Oracle Identity Navigator to discover and launch Consoles for Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager from within the Oracle Identity Navigator user interface

17.8.2 Components Deployed

Performing the configuration in this section deploys the following:

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

17.8.3 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 and Oracle Adaptive Access Manager. For more information, see Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU).
- Installation and configuration of Oracle Adaptive Access Manager with Oracle Identity Navigator in a new WebLogic domain, as described in OAAM in a New WebLogic Domain.

17.8.4 Procedure

Perform the following steps to configure Oracle Access Manager in an Oracle Identity Management domain that has Oracle Adaptive Access Manager and Oracle Identity Navigator installed:

1. Ensure that all prerequisites, listed in Prerequisites, are satisfied. In addition, see Important Notes Before You Begin.

2. Configure Oracle Adaptive Access Manager and Oracle Identity Navigator in a new WebLogic domain, as described in OAAM in a New WebLogic Domain. A new WebLogic domain to support 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.
3. 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.
4. On the Welcome screen, select the **Extend an existing WebLogic domain** option. Click **Next**.
5. On the Select a WebLogic Domain Directory screen, browse to the directory that contains the WebLogic domain in which you configured Oracle Adaptive Access Manager and Oracle Identity Navigator. Click **Next**. The Select Extension Source screen appears.
6. On the Select Extension Source screen, select the **Oracle Access Manager with Database Policy Store - 11.1.1.3.0 [Oracle_IDM2]** domain configuration option.
7. After selecting the domain configuration options, click **Next**. The Configure JDBC Data Sources Screen is displayed. Configure the `oamDS` data source, as required. After the test succeeds, the Configure JDBC Component Schema screen is displayed.
8. On the Configure JDBC Component Schema screen, select a component schema, such as the OAAM Admin Server Schema, the OAAM Admin MDS Schema, the User Messaging Service Schema, the OWSM MDS Schema, the OIM MDS 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 **Managed Servers, Clusters, and Machines** and **Deployments and Services**. 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.

     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.

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

Your existing domain with Oracle Adaptive Access Manager and Oracle Identity Navigator is extended to support Oracle Access Manager.

17.9 Starting the Servers

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

17.10 Optional Post-Installation Tasks

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

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

For more information, see the "Getting Started with Administering Oracle Access Manager" chapter in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager*.

17.11 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.

17.12 Setting Up OAM Agents

You can set up either Oracle HTTP Server WebGate or mod_OSSO as an Agent for Oracle Access Manager (OAM). Setting up an Agent involves the following steps:

1. Installing and Configuring the Agent (WebGate or mod_osso)
2. Registering the Agent as a Partner Application
3. Restarting the WebLogic Managed Servers

17.12.1 Setting Up Oracle HTTP Server WebGate

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

17.12.1.1 Installing and Configuring WebGate

To install and configure Oracle HTTP Server WebGate, complete the following steps:

1. Install Oracle HTTP Server 11g WebGate for Oracle Access Manager, as described in Installing and Configuring Oracle HTTP Server 11g Webgate for OAM.
2. Complete the post-installation steps and the registration setup, as described in Post-Installation Steps and Getting Started with a New Oracle HTTP Server 11g Webgate Agent for Oracle Access Manager.

17.12.1.2 Registering WebGate as a Partner Application

For information about registering WebGate as a Partner Application, refer to the "Agent Registration" topic and the "Managing Agents: OAM (WebGate) and OSSO (mod_osso)" chapter in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager*. Note that the Administration Server must be up and running when you are registering WebGate as a Partner Application.

17.12.1.3 Restarting Managed Servers

For information about restarting Managed Servers, see Starting the Stack.

17.12.2 Setting Up the OSSO Agent

OSSO Agent (mod_osso) is used by Oracle HTTP Server to check for an existing, valid Oracle HTTP Server cookie. If necessary, it redirects to the Oracle Access Manager runtime server to communicate with the directory during authentication. In addition, it decrypts the encrypted user identity populated by the OSSO server and sets the headers with user attributes.

17.12.2.1 Installing mod_osso

To install mod_osso, complete the following steps:

1. Install the latest version of Oracle HTTP Server. For information about installing the Web Tier, including Oracle HTTP Server, see Installing and Configuring Oracle HTTP Server 11g (11.1.1.2.0 or 11.1.1.3.0).
2. After patching your Oracle Web Tier software to the latest version, run the configuration tool to configure Oracle HTTP Server.

   On UNIX operating systems:

   ```
   <Web_Tier_ORACLE_HOME>/bin/config.sh
   ```

   On Windows operating systems:

```
<Web_Tier_ORACLE_HOME>\bin\config.bat
```

For complete instructions, go to "Configuring Your Components" in *Oracle Fusion Middleware Installation Guide for Oracle Web Tier*.

Note: After you configure Oracle HTTP Server, a working instance of Oracle HTTP Server is configured in an Instance Home.

---

3. Copy the `mod_osso.conf` file from the `<ORACLE_INSTANCE>/config/OHS/<OHS_INSTANCE>/disabled` directory to the `<ORACLE_INSTANCE>/config/OHS/<OHS_INSTANCE>/moduleconf` directory.
4. Register mod_osso as a Partner Application.

   For information about registering mod_osso as a Partner Application, refer to the "Agent Registration" topic and the "Managing Agents: OAM (WebGate) and OSSO (mod_osso)" chapter in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager*. Note that the Administration Server must be up and running when you are registering mod_osso as a Partner Application.
5. Edit the `mod_osso.conf` file to update the location of the `osso.conf` file as follows:

```
<IfModule osso_module>
                OssoIpCheck off
                OssoIdleTimeout off
                OssoSecureCookies off
                OssoConfigFile <location of the osso.conf>
              <Location>
                    require valid-user
                    AuthType Osso
              </Location>
</IfModule osso_module>
```

6. Restart Oracle HTTP Server by running the `restartproc` command in Oracle Process Manager and Notification Server (OPMN) or by using Oracle Fusion Middleware Control.

17.12.2.2 Restarting Managed Servers

For information about restarting Managed Servers, see Starting the Stack.

17.13 Setting Up Integration with OIM

For information about setting up integration between Oracle Access Manager and Oracle Identity Manager (OIM), see the chapter Integration Between OIM and OAM.

17.14 Getting Started with OAM After Installation

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

18

Configuring Oracle Adaptive Access Manager

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

18.1 Prerequisites

The following are the prerequisites for installing and configuring Oracle Identity Management 11*g* Release 1 (11.1.1.3.0) products:

1. Installing Oracle Database, as described in Installing Oracle Database.
2. Installing 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.
3. Creating and loading schemas using Oracle Fusion Middleware Repository Creation Utility (RCU), as described in Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU).
4. Installing the Oracle Identity Management 11*g* Release 1 (11.1.1.3.0) suite, as described in Installing OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0). The Oracle Identity Management suite contains Oracle Identity Manager (OIM), Oracle Access Manager (OAM), Oracle Adaptive Access Manager (OAAM), Oracle Authorization Policy Manager (OAPM), and Oracle Identity Navigator (OIN).

18.2 Important Notes Before You Begin

Before you start installing and configuring Oracle Identity Management products in any of the scenarios discussed in this chapter, keep the following points in mind:

It is assumed that you are installing Oracle Internet Directory, Oracle Virtual Directory, Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Navigator on the same machine.

Note: In this chapter, two IDM_Home directories are mentioned in descriptions and procedures. 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 document. You can specify any name for either of your IDM_Home directories. In addition, you can install the two Oracle Identity Management suites (one containing Oracle Internet Directory, Oracle Virtual Directory, Oracle Directory Services Manager, Oracle Directory Integration Platform, and Oracle Identity Federation; another containing Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Authorization Policy Manager, and Oracle Identity Navigator) 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.

If you have not installed Oracle Internet Directory, Oracle Virtual Directory, Oracle Directory Services Manager, Oracle Directory Integration Platform, or Oracle Identity Federation on the same machine where you are installing Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Authorization Policy Manager, and Oracle Identity Navigator, then you will see a single IDM_Home directory, such as **Oracle_IDM1**, under your MW_HOME directory.

For more information, see Overview and Structure of Oracle Identity Management 11g Installation.

18.3 Installing OAAM

Oracle Adaptive Access Manager (OAAM) is included in the Oracle Identity Management 11*g* Release 1 (11.1.1.3.0) Suite. You can use the Oracle Identity Management 11*g* Installer to install the Oracle Identity Management Suite. For more information, see Preparing to Install Oracle Identity Management and Installing OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0).

18.4 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

18.4.1 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.

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

18.4.2 Components Deployed

Performing the configuration in this section deploys the following:

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

18.4.3 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. For more information about schemas specific to Oracle Adaptive Access Manager, see Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU).

18.4.4 Procedure

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

1. Ensure that all prerequisites, listed in Prerequisites, are satisfied. In addition, see Important Notes Before You Begin.
2. 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.
3. On the Welcome screen, select the **Create a new WebLogic domain** option. Click **Next**. The Select Domain Source screen appears.

4. On the Select Domain Source screen ensure that the **Generate a domain configured automatically to support the following products:** option is selected. Select **Oracle Adaptive Access Manager Admin Server - 11.1.1.3.0 [Oracle_IDM2]**, which is mandatory.

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

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

5. Enter a name and a location for the domain to be created, and click **Next**. The Configure Administrator User Name and Password screen appears.
6. Configure a user name and a password for the administrator. The default user name is `weblogic`. Click **Next**.
7. Choose `JRockit SDK 160_17_R28.0.0-679` 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.
8. On the Configure JDBC Component Schema screen, select a component schema, such as the OAAM Admin Server Schema or the OAAM Admin MDS Schema, that you want to modify.

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

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

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, 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.

18.5 OAAM in a Domain Containing OAM, OIM, and OIN

This topic describes how to configure Oracle Adaptive Access Manager (OAAM) in an existing Oracle Identity Management domain that contains Oracle Access Manager (OAM), Oracle Identity Manager (OIM), and Oracle Identity Navigator (OIN).

It includes the following sections:

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure

18.5.1 Appropriate Deployment Environment

Perform the configuration in this topic if you want to install Oracle Adaptive Access Manager in an environment where you may want to set up integration between Oracle Identity Manager and Oracle Adaptive Access Manager. You may use Oracle Access Manager for Single Sign-On and access management. Oracle Identity Navigator enables you to discover and launch Consoles for these products from within the Oracle Identity Navigator user interface.

18.5.2 Components Deployed

Performing the configuration in this section deploys the following:

- Managed Server for Oracle Adaptive Access Manager
- Oracle Adaptive Access Manager Console on the existing Administration Server

18.5.3 Dependencies

The configuration in this section depends on the following:

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

18.5.4 Procedure

To configure Oracle Adaptive Access Manager in an existing Oracle Identity Management domain that contains Oracle Access Manager, Oracle Identity Manager, and Oracle Identity Navigator, complete the following steps:

1. Ensure that all prerequisites, listed in Prerequisites, are satisfied. In addition, see Important Notes Before You Begin.
2. Ensure that Oracle Access Manager, Oracle Identity Manager, and Oracle Identity Navigator are configured in a new WebLogic domain, as described in OIM, OAM, and OIN in a New WebLogic Domain.
3. 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.
4. On the Welcome screen, select the **Extend an existing WebLogic domain** option. Click **Next**.
5. On the Select a WebLogic Domain Directory screen, browse to the domain directory that contains Oracle Access Manager, Oracle Identity Manager, and Oracle Identity Navigator. Click **Next**. The Select Domain Source screen appears.
6. On the Select Extension Source screen, ensure that the **Extend my domain automatically to support the following products:** option is selected. Select **Oracle Adaptive Access Manager Admin Server - 11.1.1.3.0 [Oracle_IDM2]**, which is mandatory.

   When you select the **Oracle Adaptive Access Manager Admin Server - 11.1.1.3.0 [Oracle_IDM2]** option, the **Oracle Identity Navigator - 11.1.1.3.0 [Oracle_IDM2]** option is also selected, by default.

   In addition, you can select **Oracle Adaptive Access Manager - Server - 11.1.1.3.0 [Oracle_IDM2]**, which is optional. Click **Next**. The Configure JDBC Component Schema screen appears.

   The screen lists the following component schemas:

   - SOA Infrastructure
   - OAAM Admin Schema
   - User Messaging Service
   - OAAM Admin MDS Schema
   - OIM MDS Schema
   - OWSM MDS Schema
   - SOA MDS Schema
   - OIM Schema
7. 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.
8. 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**.
9. Optional: Configure Managed Servers, as required.

10. 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*.

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

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

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

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

14. Optional: Select Deployments, such as applications and libraries, and Services to target them to a particular cluster or server, such as `oaam_server1` (default value).

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

    Your existing Oracle Identity Management domain with Oracle Access Manager, Oracle Identity Manager, and Oracle Identity Navigator is extended to support Oracle Adaptive Access Manager.

18.6 Starting the Servers

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

Note: If you are upgrading from Oracle Adaptive Access Manager 10*g* to Oracle Adaptive Access Manager 11*g*, do not start Oracle Adaptive Access Manager Managed Servers until you have performed the Oracle Adaptive Access Manager Middle Tier Upgrade using the Upgrade Assistant tool. For more information, see the *Oracle Fusion Middleware Upgrade Guide for Oracle Identity Management*.

18.7 Post-Installation Steps

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

1. Create Oracle WebLogic Server Users as follows:

   a. Log in to the Oracle WebLogic Administration Console for your WebLogic administration domain.

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

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

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

   e. Assign the user `user1` to any of the newly created groups with the OAAM prefix.

2. Set up and back up Oracle Adaptive Access Manager Encryption Keys, as described in the "Setting Up Encryption and Database Credentials for OAAM" topic in the *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*. Ensure that you have a backup of the Oracle Adaptive Access Manager Encryption Keys; they are required if you want to re-create the Oracle Adaptive Access Manager domain.
3. Import Policies as follows:
   a. Ensure that you have downloaded the policies.
   b. Log in to the Oracle Adaptive Access Manager Administration (OAAM_ADMIN) using the following URL: `http://<host>:<port>/oaam_admin`
   c. Click the **Policy** tab, and then click **Import Policies**. The default policies are located in the `<Oracle_IDM2>/oaam/init` directory.

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

4. Import Knowledge Based Authentication (KBA) questions as follows:
   a. Log in to the Oracle Adaptive Access Manager Administration (OAAM_ADMIN) using the following URL: `http://<host>:<port>/oaam_admin`
   b. Click the **KBA Questions** tab, and then click **Import KBA**. The default questions are located in the `<Oracle_IDM2>/oaam/kba_questions` directory. You must load questions for the languages you want to support.
5. Load Location Data into the Oracle Adaptive Access Manager database as follows:
   a. Configure the IP Location Loader script, as described in the topics "OAAM Command Line Interface Scripts" and "Importing IP Location Data" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*.
   b. Make a copy of the `sample.bharosa_location.properties` file, which is located under the `oaam/WEB-INF/classes/` directory. Enter location data details in the location.data properties, as in the following examples:

      ```
      location.data.provider=quova

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

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

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

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

      On Windows: `loadIPLocationData.bat`

      On UNIX: `./loadIPLocationData.sh`

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

18.8 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 Servers.

   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`

18.9 Migrating Policy and Credential Stores

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

Migrating policy and credential stores involves the following steps:

1. Creating JPS Root
2. Reassociating the Policy and Credential Store

18.9.1 Creating JPS Root

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

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

   ```
   dn: cn=jpsroot_idm
   cn: jpsroot_idm_idm
   objectclass: top
   objectclass: orclcontainer
   ```

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

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

18.9.2 Reassociating the Policy and Credential Store

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

1. From IDMHOST1, start the `wlst` shell from the *ORACLE_HOME*`/common/bin` directory. For example:

   ```
   ./wlst.sh
   ```

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

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

   For example:

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

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

   Syntax:

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

   For example:

   ```
   wls:/IDMDomain/serverConfig> reassociateSecurityStore(domain="IDMDomain",
   admin="cn=orcladmin",password="password",
   ldapurl="ldap://oid.mycompany.com:389",servertype="OID",
   jpsroot="cn=jpsroot_idm_idmhost1")
   ```

   The output for the command is as follows:

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

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

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

4. Restart the Administration Server after the command completes successfully. For information about restarting the Administration Server, see Starting the Servers.

18.10 Getting Started with OAAM After Installation

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

19

OAM and OAAM Joint Domain Configuration Scenarios

This chapter explains how to configure Oracle Access Manager (OAM) and Oracle Adaptive Access Manager (OAAM) with other Oracle Identity Management components, such as Oracle Identity Manager (OIM) and Oracle Identity Navigator (OIN), in a new or existing WebLogic domain. It includes the following topics:

19.1 Prerequisites

The following are the prerequisites for installing and configuring Oracle Identity Management 11*g* Release 1 (11.1.1.3.0) products:

1. Installing Oracle Database, as described in Installing Oracle Database.
2. Installing 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.
3. **For Oracle Identity Manager users only**: Installing Oracle SOA Suite 11*g* Release 1 (11.1.1.2.0) and patching it to 11.1.1.3.0, as described in Installing the Latest Version of Oracle SOA Suite (Oracle Identity Manager Users Only).
4. Creating and loading schemas using Oracle Fusion Middleware Repository Creation Utility (RCU), as described in Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU).
5. Installing the Oracle Identity Management 11*g* Release 1 (11.1.1.3.0) suite, as described in Installing OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0). The Oracle Identity Management suite contains Oracle Identity Manager (OIM), Oracle Access Manager (OAM), Oracle Adaptive Access Manager (OAAM), Oracle Authorization Policy Manager (OAPM), and Oracle Identity Navigator (OIN).

19.2 Important Notes Before You Begin

Before you start installing and configuring Oracle Identity Management products in any of the scenarios discussed in this chapter, keep the following points in mind:

It is assumed that you are installing Oracle Internet Directory, Oracle Virtual Directory, Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Navigator on the same machine.

Note: In this chapter, two IDM_Home directories are mentioned in descriptions and procedures. 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 document. You can specify any name for either of your IDM_Home directories. In addition, you can install the two Oracle Identity Management suites (one containing Oracle Internet Directory, Oracle Virtual Directory, Oracle Directory Services Manager, Oracle Directory Integration Platform, and Oracle Identity Federation; another containing Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Authorization Policy Manager, and Oracle Identity Navigator) 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.

If you have not installed Oracle Internet Directory, Oracle Virtual Directory, Oracle Directory Services Manager, Oracle Directory Integration Platform, or Oracle Identity Federation on the same machine where you are installing Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Authorization Policy Manager, and Oracle Identity Navigator, then you will see a single IDM_Home directory, such as **Oracle_IDM1**, under your MW_HOME directory.

For more information, see Overview and Structure of Oracle Identity Management 11g Installation.

19.3 Installing Oracle Identity Management 11*g* Release 1 (11.1.1.3.0)

You can use the Oracle Identity Management 11*g* Installer to install the Oracle Identity Management 11*g* Release 1 (11.1.1.3.0) suite that contains Oracle Access Manager (OAM), Oracle Identity Manager (OIM), Oracle Adaptive Access Manager (OAAM), Oracle Authorization Policy Manager (OAPM), and Oracle Identity Navigator (OIN). For more information, see Preparing to Install Oracle Identity Management and Installing OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0).

19.4 OAM, OIM, and OIN in a New WebLogic Domain

This topic describes how to configure Oracle Access Manager (OAM), Oracle Identity Manager (OIM), and Oracle Identity Navigator (OIN) in a new WebLogic administration domain. It includes the following sections:

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure

19.4.1 Appropriate Deployment Environment

Perform the configuration in this topic if you want to install Oracle Access Manager, Oracle Identity Manager, and Oracle Identity Navigator together in an environment. You can also set up integration between Oracle Identity Manager and Oracle Access Manager, as described in Integration Between OIM and OAM.

19.4.2 Components Deployed

Performing the installation and configuration in this section deploys the following:

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

19.4.3 Dependencies

The installation and configuration in this section depends on the following:

- Oracle WebLogic Server.
- Complete installation of the Oracle Identity Management 11*g* software.
- Installation of Oracle SOA Suite
- Database schemas for Oracle Identity Manager, Oracle SOA Suite, and Oracle Access Manager. For more information about schemas specific to Oracle Identity Manager and Oracle Access Manager, see Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU).

19.4.4 Procedure

Perform the following steps to install and configure Oracle Access Manager, Oracle Identity Manager, and Oracle Identity Navigator in a new WebLogic administration domain:

1. Ensure that all the prerequisites, listed in Prerequisites, are satisfied. In addition, see Important Notes Before You Begin.
2. Run the `<Oracle_IDM2>/common/bin/config.sh` script. (`<Oracle_IDM2>\common\bin\config.cmd` on Windows). The Oracle Fusion Middleware Configuration Wizard appears.

3. On the Welcome screen, select the **Create a new WebLogic domain** option. Click **Next**. The Select Domain Source screen is displayed.
4. On the Select Domain Source screen, select the **Generate a domain configured automatically to support the following products:** option.
5. Select the following domain configuration options:
   - **Oracle Access Manager with Database Policy Store - 11.1.1.3.0 [Oracle_IDM2]**

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

   - **Oracle Identity Navigator - 11.1.1.3.0 [Oracle_IDM2]**
   - **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]**.
6. After selecting the domain configuration options, click **Next**. The Specify Domain Name and Location screen is displayed.
7. 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.
8. 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.
9. Choose `JRockit SDK 160_17_R28.0.0-679` and Production Mode in the Configure Server Start Mode and JDK screen of the Oracle Fusion Middleware Configuration Wizard. Click **Next**. The Configure JDBC Data Sources Screen is displayed. Configure the `oamDS` data source, as required. After the test succeeds, the Configure JDBC Component Schema screen is displayed.
10. On the Configure JDBC Component Schema screen, select a component schema, such as the OIM Infrastructure Schema, the SOA Infrastructure Schema, the User Messaging Service Schema, the OWSM MDS Schema, the OIM MDS 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.
11. On the Select Optional Configuration screen, you can configure **Administration Server, Managed Servers, Clusters, and Machines**, **Deployments and Services**, **JMS File Store**, and **RDBMS Security 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 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.

  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.
- Optional: Configure RDBMS Security Store, 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 Identity Manager, Oracle 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.
13. Start the Oracle Identity Manager Configuration Wizard, as described in Starting the Oracle Identity Manager 11g Configuration Wizard.
14. Configure Oracle Identity Manager Server, as described in Configuring OIM Server.
15. 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.

19.5 OAM, OAAM, and OIN in a New WebLogic Domain

This topic describes how to configure Oracle Access Manager (OAM), Oracle Adaptive Access Manager (OAAM), and Oracle Identity Navigator (OIN) together in a new WebLogic administration domain. It includes the following sections:

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure

19.5.1 Appropriate Deployment Environment

Perform the configuration in this topic if you want to install Oracle Access Manager, Oracle Access Manager, and Oracle Identity Navigator together in an environment.

19.5.2 Components Deployed

Performing the installation and configuration in this section deploys the following:

- Administration Server
- Managed Servers for Oracle Access Manager and Oracle Adaptive Access Manager
- Oracle Access Manager Console, Oracle Adaptive Access Manager Console, and Oracle Identity Navigator application on the Administration Server

19.5.3 Dependencies

The installation and configuration in this section depends on the following:

- Oracle WebLogic Server.
- Complete installation of the Oracle Identity Management 11*g* software.
- Database schemas for Oracle Access Manager and Oracle Adaptive Access Manager. For more information about schemas specific to Oracle Adaptive Access Manager and Oracle Access Manager, see Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU).

19.5.4 Procedure

Perform the following steps to install and configure Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Navigator in a new WebLogic administration domain:

1. Ensure that all the prerequisites, listed in Prerequisites, are satisfied. In addition, see Important Notes Before You Begin.
2. Run the `<Oracle_IDM2>/common/bin/config.sh` script. (`<Oracle_IDM2>\common\bin\config.cmd` on Windows). The Oracle Fusion Middleware Configuration Wizard appears.
3. On the Welcome screen, select the **Create a new WebLogic domain** option. Click **Next**. The Select Domain Source screen is displayed.
4. On the Select Domain Source screen, select the **Generate a domain configured automatically to support the following products:** option.
5. Select the following domain configuration options:
   - **Oracle Access Manager with Database Policy Store - 11.1.1.3.0 [Oracle_IDM2]**

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

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

- **Oracle Adaptive Access Manager Admin Server - 11.1.1.3.0 [Oracle_IDM2]**, which is mandatory.

  and

  Optionally, **Oracle Adaptive Access Manager - Server - 11.1.1.3.0 [Oracle_IDM2]**

Note: When you select the **Oracle Adaptive Access Manager - Server - 11.1.1.30 [Oracle_IDM2]** option, the **Oracle WSM Policy Manager - 11.1.1.0 [oracle_common]** option is also selected, by default.

When you select the **Oracle Adaptive Access Manager Admin Server - 11.1.1.3.0 [Oracle_IDM2}** option, the **Oracle Identity Navigator - 11.1.1.3.0 [Oracle_IDM2]** option is also selected, by default.

---

6. After selecting the domain configuration options, click **Next**. The Specify Domain Name and Location screen is displayed.
7. On the Specify Domain Name and Location screen, enter a name and location for the domain to be created. Click **Next**. The Configure Administrator User Name and Password screen is displayed.
8. 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.
9. Choose `JRockit SDK 160_17_R28.0.0-679` and Production Mode in the Configure Server Start Mode and JDK screen of the Oracle Fusion Middleware Configuration Wizard. Click **Next**. The Configure JDBC Data Sources Screen is displayed. Configure the `oamDS` data source, as required. After the test succeeds, the Configure JDBC Component Schema screen is displayed.
10. On the Configure JDBC Component Schema screen, select a component schema, such as the OAAM Admin Server Schema, the OAAM Admin MDS Schema, that you want to modify.

    You can set values for Schema Owner, Schema Password, Database and Service, Host Name, and Port. Click **Next**. The Test JDBC Component Schema screen appears. After the test succeeds, the Select Optional Configuration screen appears.
11. On the Select Optional Configuration screen, you can configure **Administration Server, Managed Servers, Clusters, and Machines**, **Deployments and Services**, and **RDBMS Security 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 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.

  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.

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 Adaptive Access Manager, Oracle 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.

19.6 Starting the Servers

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

19.7 Getting Started with OAM After Installation

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

19.8 Getting Started with OAAM After Installation

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

20

Configuring Oracle Authorization Policy Manager

This chapter explains how to configure Oracle Authorization Policy Manager (OAPM) in a new or existing WebLogic administration domain.

It discusses the following topics:

- Prerequisites
- Important Notes Before You Begin
- Installing OAPM
- OAPM in a New WebLogic Domain
- OAPM in a Domain Containing OIM
- OAPM in a Domain Containing OIM, OAM, OAAM, and OIN
- Starting the Servers
- Reassociating WebLogic Server with LDAP
- Verifying the OAPM Installation
- Getting Started with OAPM After Installation

20.1 Prerequisites

The following are the prerequisites for installing and configuring Oracle Identity Management 11*g* Release 1 (11.1.1) products:

1. Installing Oracle Database, as described in Installing Oracle Database.
2. Installing 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.
3. Creating and loading schemas using Oracle Fusion Middleware Repository Creation Utility (RCU), as described in Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU).
4. Installing the Oracle Identity Management 11*g* Release 1 (11.1.1.3.0) suite, as described in Installing OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0). The Oracle Identity Management suite contains Oracle Identity Manager (OIM), Oracle Access Manager (OAM), Oracle Adaptive Access Manager (OAAM), Oracle Authorization Policy Manager (OAPM), and Oracle Identity Navigator (OIN).

20.2 Important Notes Before You Begin

Before you start installing and configuring Oracle Identity Management products in any of the scenarios discussed in this chapter, keep the following points in mind:

It is assumed that you are installing Oracle Internet Directory, Oracle Virtual Directory, Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Navigator on the same machine.

Note: In this chapter, two IDM_Home directories are mentioned in descriptions and procedures. 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 document. You can specify any name for either of your IDM_Home directories. In addition, you can install the two Oracle Identity Management suites (one containing Oracle Internet Directory, Oracle Virtual Directory, Oracle Directory Services Manager, Oracle Directory Integration Platform, and Oracle Identity Federation; another containing Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Authorization Policy Manager, and Oracle Identity Navigator) 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.

If you have not installed Oracle Internet Directory, Oracle Virtual Directory, Oracle Directory Services Manager, Oracle Directory Integration Platform, or Oracle Identity Federation on the same machine where you are installing Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Authorization Policy Manager, and Oracle Identity Navigator, then you will see a single IDM_Home directory, such as **Oracle_IDM1**, under your MW_HOME directory.

For more information, see Overview and Structure of Oracle Identity Management 11g Installation.

20.3 Installing OAPM

You must run the Oracle Identity Management 11*g* Installer to install Oracle Authorization Policy Manager (OAPM). For more information, see Preparing to Install Oracle Identity Management and Installing OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0).

20.4 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

20.4.1 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 Navigator, or Oracle Adaptive Access Manager at a later stage in the same domain.

20.4.2 Components Deployed

Performing the configuration in this section deploys the following:

- WebLogic Administration Server
- Oracle Authorization Policy Manager application on the Administration Server

20.4.3 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). For more information about schemas specific to Oracle Authorization Policy Manager, see Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU).

20.4.4 Procedure

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

1. Ensure that all the prerequisites, listed in Prerequisites, are satisfied. In addition, see Important Notes Before You Begin.
2. 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.
3. On the Welcome screen, select the **Create a new WebLogic domain** option. Click **Next**. The Select Domain Source screen appears.
4. On the Select Domain Source screen, ensure that the **Generate a domain configured automatically to support the following products:** option is selected.

   Select the **Oracle Application Authorization Policy Manager - 11.1.1.3.0 [Oracle_IDM2]** 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.

5. Enter a name and a location for the domain to be created, and click **Next**. The Configure Administrator User Name and Password screen appears.
6. Configure a user name and a password for the administrator. The default user name is `weblogic`. Click **Next**.
7. Choose `JRockit SDK 160_17_R28.0.0-679` 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.
8. 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.
9. On the Select Optional Configuration screen, you can configure the **Administration Server**, **Managed Servers**, **Clusters**, **Machines**, **Deployments and Services**, and **RDBMS Security Store**. Select the relevant check boxes and click **Next**.
   - 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.

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

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 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.

20.5 OAPM in a Domain Containing OIM

This topic describes how to configure Oracle Authorization Policy Manager (OAPM) in an existing Oracle Identity Management domain that has Oracle Identity Manager (OIM) installed and configured.

It includes the following sections:

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure
- Post-Configuration Steps

20.5.1 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 and Oracle SOA Suite are already installed and configured. Note that Oracle Identity Manager requires Oracle SOA Suite. You may install other Oracle Identity Management products, such as Oracle Access Manager, Oracle Identity Navigator, and Oracle Adaptive Access Manager at a later time in the same domain. You can discover and launch Consoles for Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Authorization Policy Manager from within the Oracle Identity Navigator user interface.

20.5.2 Components Deployed

Performing the configuration in this section deploys the Oracle Authorization Policy Manager application on the existing WebLogic Administration Server.

20.5.3 Dependencies

The configuration in this section depends on the following:

- Oracle WebLogic Server.
- Installation of the Oracle Identity Management 11*g* software.
- Oracle SOA Suite (required by Oracle Identity Manager).
- Database schemas for Oracle Authorization Policy Manager and Metadata Services (MDS), Oracle Identity Manager, and Oracle SOA Suite. For more information, see Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU).

20.5.4 Procedure

To configure Oracle Authorization Policy Manager in an existing WebLogic domain that has Oracle Identity Manager configured, complete the following steps:

1. Ensure that all the prerequisites, listed in Prerequisites, are satisfied. In addition, see Important Notes Before You Begin.
2. Run the `<Oracle_IDM2>/common/bin/config.sh` (on UNIX) script. (`<Oracle_IDM2>\common\bin\config.cmd` on Windows). The Oracle Fusion Middleware Configuration Wizard appears.
3. Configure Oracle Identity Manager in a new WebLogic domain, as described in OIM Without LDAP Sync in a New Domain.
4. Ensure that the WebLogic domain with Oracle Identity Manager is configured correctly. After the domain configuration is complete, on the Creating Domain screen, click **Done** to dismiss the Oracle Fusion Middleware 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.
5. 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.
6. On the Welcome screen, select the **Extend an existing WebLogic domain** option. Click **Next**.
7. On the Select a WebLogic Domain Directory screen, browse to the `<MW_HOME>/user_projects/domains` directory that contains your Oracle Identity Manager domain. Click **Next**. The Select Extension Source screen appears.
8. 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 [Oracle_IDM2]**. Click **Next**. The Configure JDBC Component Schema screen appears.
9. 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
   - User Messaging Service
   - APM MDS Schema
   - APM 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.
10. 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.

  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, such as `oam_server1` (default value).
- Optional: Configure JMS File Stores, as required.

11. On the Configuration Summary screen, review the domain configuration, and click **Extend** to start extending the Oracle Identity Manager domain to support Oracle Authorization Policy Manager.

    Your existing WebLogic domain with Oracle Identity Manager is extended to support Oracle Authorization Policy Manager.

20.5.5 Post-Configuration Steps

You must complete the following steps after configuring Oracle Authorization Policy Manager in an Oracle Identity Manager domain:

1. Browse to the `<Extended_Domain_Home>/config/fmwconfig` directory.
2. Open the `jps-config.xml` file in a text editor. Be sure to back up the file before making any changes.
3. Search for the `jpscontexts` section, with the name `default`, in the file. The section looks like the following:

```
<jpsContexts name="default">
        <!-- This is the default JPS context. All the mendatory services and
Login Modules must be configured in this default context -->
        <jpsContext name="default">
            <serviceInstanceRef ref="credstore"/>
            <serviceInstanceRef ref="keystore"/>
            <serviceInstanceRef ref="policystore.xml"/>
            <serviceInstanceRef ref="audit"/>
    <serviceInstanceRef ref="idstore.oim"/>
</jpsContext>
```

4. Change the last serviceInstance reference entry from `<serviceInstanceRef ref="idstore.oim"/>` to `<serviceInstanceRef ref="idstore.ldap"/>`.
5. Copy the entire `jpscontexts` section and paste it after the default `jpscontexts` section. Modify the `default` entry and the `serviceInstance` reference entry in the new section as follows:

```
<jpsContexts default="oim">
        <!-- This is the default JPS context. All the mendatory services and
Login Modules must be configured in this default context -->
        <jpsContext name="default">
            <serviceInstanceRef ref="credstore"/>
            <serviceInstanceRef ref="keystore"/>
            <serviceInstanceRef ref="policystore.xml"/>
            <serviceInstanceRef ref="audit"/>
    <serviceInstanceRef ref="idstore.oim"/>
</jpsContext>
```

6. Save the `jps-config.xml` file after making the changes.
7. Open the Oracle Enterprise Manager MBean browser after logging in to Oracle Enterprise Manager Fusion Middleware Control
8. Open the `domain oracle.as.soainfra.config`.
9. Select on the following in order:
   - `WorkflowIdentityConfig -> human-workflow ->`
   - `WorkflowIdentityConfig.ConfigurationType -> jazn.com ->`
   - `WorkflowIdentityConfig.ConfigurationType.ProviderType -> JpsProvider ->`
   - `WorkflowIdentityConfig.ConfigurationType.ProviderType.PropertyType -> jpsContextName`
10. Change the value of the `jpsContextName` property to the `oim` context created in the `jps-config.xml` file, as in Step 5. Click the `setValue` operation, and change the value to `oim`.
11. Restart the Administration Server and all Managed Servers for the changes to take effect, as described in Starting the Servers.

20.6 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

20.6.1 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.

20.6.2 Components Deployed

Performing the configuration in this section deploys the Oracle Authorization Policy Manager application on the existing WebLogic Administration Server.

20.6.3 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. For more information about schemas specific to Oracle Authorization Policy Manager, see Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU).

20.6.4 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 Navigator, complete the following steps:

1. Ensure that all the prerequisites, listed in Prerequisites, are satisfied. In addition, see Important Notes Before You Begin.
2. 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.
3. Create a new WebLogic domain to support Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Navigator. For more information, see Simultaneous configuration of OIN, OAPM, OAAM, OAM, and OIM.

   Note: On the Select Domain Source screen, do not select the **Oracle Authorization Policy Manager - 11.1.1.3.0 [Oracle_IDM2]** option.

4. Ensure that the WebLogic domain with Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Navigator is configured correctly. After the domain configuration is complete, on the Creating Domain screen, 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.
5. 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.

6. On the Welcome screen, select the **Extend an existing WebLogic domain** option. Click **Next**.
7. 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.
8. 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 [Oracle_IDM2]**. Click **Next**. The Configure JDBC Component Schema screen appears.
9. 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.
10. 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.

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, such as `oam_server1` (default value).
- Optional: Configure JMS File Stores, as required.

11. 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.

20.7 Starting the Servers

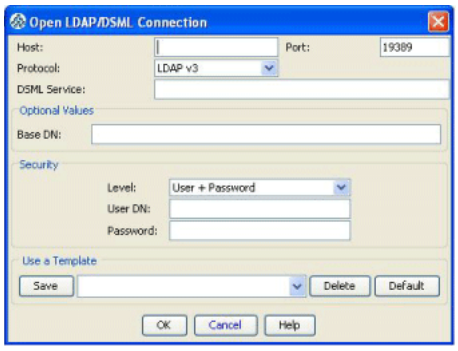
After installing and configuring Oracle Authorization Policy Manager, you must run the Oracle WebLogic Administration Server, as described in Starting or Stopping the Oracle Stack.

20.8 Reassociating WebLogic Server with LDAP

After installing and configuring Oracle Authorization Policy Manager, you must reassociate Oracle WebLogic Server with LDAP as follows:

1. Ensure that the WebLogic Administration Server is up and running. For information about starting the WebLogic Administration Server, see Starting or Stopping the Oracle Stack.
2. Use an LDAP browser or client, such as JXplorer, to add a new node on the LDAP server that Oracle WebLogic Server is going to associate with:
   a. On the **File** menu in your LDAP browser, click **Connect** to connect to your LDAP server. The Open LDAP/DSML Connection screen appears.

Figure 20–1 Connecting to an LDAP Server LD



   b. In the **Host** text box, enter the host name of your LDAP server.
   c. In the **Port** text box, enter the port number.
   d. On the **Level** drop-down list, choose the **User + Password** option.

e. In the **User DN** text box, enter the base distinguished name of the directory to which you want to connect.

f. In the **Password** text box, enter the password. Click **OK**. If the connection is successful, a list of entries in the Directory Information Tree is displayed in the left navigation pane.

g. Select the parent entry. From the **Edit** menu, choose **New**. The Set Entry Object Classes screen appears.

h. Select the **Suggest Classes** check box if you want to view the compulsory object classes for the new entry.

i. Verify that the Distinguished Name of the parent entry in the **Parent DN** text box is correct.

j. In the **Enter RDN** text box, enter the Relative Distinguished Name of the new entry. For example, to add `apm_test_name` to the new entry, enter `cn=apm_test_name`. JXplorer displays the compulsory object classes for the new entry in the Selected Classes pane. Click **OK**.

k. If the information about the new entry is correct, click **Submit**.

3. Change the association of Oracle WebLogic Server to the new node by using WebLogic Scripting Tool (WLST) or Oracle Enterprise Manager Fusion Middleware Control:

Using WLST

a. At the command prompt, change your present working directory to the `<MW_HOME>/oracle_common/common/bin` directory.

b. Run the `wlst.sh` script.

c. At the WLS prompt, use the WLST command `reassociateSecurityStore` as follows:

```
wls> reassociateSecurityStore(domain="domainName",
admin="cnSpecification", password="passWord",
ldapurl="hostAndPort", servertype="ldapSrvrType",
jpsroot="cnSpecification" [,join="trueOrfalse"])
```

Where

Argument	Description
`domain`	Specifies the name of the domain where the reassociation occurs.
`admin`	Specifies the user name of the administrator on the LDAP server. The format is `cn=usrName`.
`password`	Specifies the password for the administrator on the LDAP server.
`ldapurl`	Specifies the Uniform Resource Identifier (URI) of the LDAP server. The format is `ldap//:host:port`.
`servertype`	Specifies the type of the target LDAP server. The only valid types are Oracle Internet Directory and Oracle Virtual Directory.
`jpsroot`	Specifies the root node in the target LDAP repository under which all data is migrated. The format is `cn=nodeName`.

Argument	Description
`join`	Specifies whether the domain shares a policy store specified in another domain. `-Optional`. This flag is set to true when an existing policy store in another domain is shared. It is set to false otherwise. Using this argument allows multiple WebLogic domains to point to the same logical policy store.

Example Usage

```
reassociateSecurityStore(domain="myDomain",
admin="cn=adminName", password="myPass",
ldapurl="ldap(s)://myhost.example.com:3060",
servertype="OID", jpsroot="cn=testNode")
```

If you want a domain other than `myDomain`, such as `yourDomain`, to share the policy store in `myDomain`, then you must run the command as follows:

```
reassociateSecurityStore(domain="yourDomain",
admin="cn=adminName", password="myPass",
ldapurl="ldap(s)://myhost.example.com:3060",
servertype="OID", jpsroot="cn=testNode", join="true")
```

Using Oracle Enterprise Manager Fusion Middleware Control

a. Log in to Oracle Enterprise Manager Fusion Middleware Control.

b. Navigate to your WebLogic domain.

c. Right-click and choose **Security** > **Security Provider Configuration**.

d. Click **Change Association**.

e. On the Set Security Provider page, in the LDAP Server Details section, select the LDAP server type, host name, port number, connection string, and password.

f. In the LDAP Root Node Details section, enter a distinguished name for the JPS root.

g. Select the **Create New Domain** option if you want to create a new policy and credential domain on LDAP.

Note: To join a specified existing domain, do not select the **Create New Domain** option.

---

h. In the **Domain Name** text box, enter a name for the domain.

i. Click **OK**.

Note: After the reassociation, CredentialStore, SystemPolicy and apm are migrated to the node. You can verify them through an LDAP management tool, such as JXplorer.

20.9 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.

20.10 Getting Started with OAPM After Installation

After installing Oracle Authorization Policy Manager (OAPM), refer to the "Getting Started with Oracle Authorization Policy Manager" chapter in the *Oracle Fusion Middleware Authorization Policy Manager Administrator's Guide*.

21

Integration Between OIM and OAM

This chapter describes how to set up integration between Oracle Identity Manager (OIM) and Oracle Access Manager (OAM).

It includes the following topics:

21.1 Overview

For an overview of Oracle Identity Management suite-level integration scenarios, see the guide *Oracle Fusion Middleware Integration Overview for Oracle Identity Management Suite*.

This chapter describes how to set up the integration using the WebLogic Server Domain Agent.

Note: However, you can migrate from the Domain Agent to Oracle HTTP Server 10*g* Webgate for Oracle Access Manager if you wish to protect partner applications outside of the WebLogic domain.

See chapter Migrating from Domain Agent to Oracle HTTP Server 10g Webgate for OAM for more information.

21.2 Important Notes Before You Begin

Before you start installing and configuring Oracle Identity Management products in any of the scenarios discussed in this chapter, keep the following points in mind:

- It is assumed that you are installing Oracle Internet Directory, Oracle Virtual Directory, Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Navigator on the same machine.

Note: In this chapter, two IDM_Home directories are mentioned in the descriptions and procedures. 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 document. You can specify any name for either of your IDM_Home directories. In addition, you can install the two Oracle Identity Management suites (one containing Oracle Internet Directory, Oracle Virtual Directory, Oracle Directory Services Manager, Oracle Directory Integration Platform, and Oracle Identity Federation; another containing Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Authorization Policy Manager, and Oracle Identity Navigator) 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.

If you have not installed Oracle Internet Directory, Oracle Virtual Directory, Oracle Directory Services Manager, Oracle Directory Integration Platform, or Oracle Identity Federation on the same machine where you are installing Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Authorization Policy Manager, and Oracle Identity Navigator, then you will see a single IDM_Home directory, such as **Oracle_IDM1**, under your MW_HOME directory.

For more information, see Overview and Structure of Oracle Identity Management 11g Installation.

- By performing the domain configuration procedures described in this chapter, you can create Managed Servers on a local machine (the machine on which the Administration Server is running). However, you can create and start Managed Servers for Oracle Identity Management components on a remote machine. For more information, see the "Creating and Starting a Managed Server on a Remote Machine" topic in the guide *Oracle Fusion Middleware Creating Templates and Domains Using the Pack and Unpack Commands*.
- You must use the Oracle Identity Manager Configuration Wizard to configure only Oracle Identity Manager Server, Oracle Identity Manager Design Console (on Windows only), and Oracle Identity Manager Remote Manager.

  You must complete this additional configuration for Oracle Identity Manager components after configuring Oracle Identity Manager in a new or existing WebLogic administration domain. For more information, see OIM Domain Configuration Scenarios.

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

during the initial setup of the Server. After the successful setup of Oracle Identity Manager Server, you cannot run the Oracle Identity Manager Configuration Wizard again to modify the configuration of Oracle Identity Manager Server. For such modifications, you must use Oracle Enterprise Manager Fusion Middleware Control.

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.

21.3 Task Roadmap

Table 21–1 Task Roadmap

Task	For More Information
Install Oracle Database	Installing Oracle Database
Create and load database schemas	Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU)
Install Oracle WebLogic Server 10.3.3 and create a Middleware Home	Installing Oracle WebLogic Server 10.3.3 and Creating the Oracle Middleware Home
Ensure that the Oracle Identity Management 11*g* Release 1 (11.1.1.3.0) suite containing Oracle Internet Directory (OID) and Oracle Virtual Directory (OVD) are installed	Installing OID, OVD, ODSM, ODIP, and OIF (11.1.1.5.0)
Configure Oracle Internet Directory (OID) and Oracle Virtual Directory (OVD) in a WebLogic administration domain	OID and OVD with ODSM in a New WebLogic Domain
On the command line, use the cd command to move from your present working directory to the following directory: On UNIX: `<WL_HOME>/server/lib` On Windows: `<WL_HOME>\server\lib`	
At the command prompt, run the following command: `<full path to the directory where java is installed>/java -jar wljarbuilder.jar`	This command generates a library, which is required by all WebLogic Server application clients.

Table 21–1 (Cont.) Task Roadmap

Task	For More Information
Install Oracle Identity Management 11*g* Release 1 (11.1.1.3.0) suite containing Oracle Identity Manager (OIM) and Oracle Access Manager (OAM)	Installing OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0)
Configure Oracle Identity Manager (OIM) and Oracle Access Manager (OAM) in a new or existing WebLogic administration domain	OIM with LDAP Sync, and OAM
Set Up Integration Between OIM and OAM Using the Domain Agent	Setting Up Integration Between OIM and OAM Using the Domain Agent
Verify the Configuration	Verifying the Configuration

21.4 Prerequisites

You must complete the following prerequisites for setting up integration between Oracle Identity Manager and Oracle Access Manager:

1. Install a supported version of Oracle Database, as described in Installing Oracle Database.
2. Create and load database schemas, as described in Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU).
3. Install Oracle WebLogic Server 10.3.3 and create a Middleware Home, as described in Installing Oracle WebLogic Server 10.3.3 and Creating the Oracle Middleware Home
4. Ensure that the Oracle Identity Management 11*g* Release 1 (11.1.1.3.0) suite containing Oracle Internet Directory (OID) and Oracle Virtual Directory (OVD) are installed, as described in Installing OID, OVD, ODSM, ODIP, and OIF (11.1.1.5.0).

   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).

   For more information, see Important Notes Before You Begin.
5. Configure Oracle Internet Directory (OID) and Oracle Virtual Directory (OVD) in a WebLogic administration domain, as described in OID and OVD with ODSM in a New WebLogic Domain.
6. On the command line, use the `cd` command to move from your present working directory to the following directory:

   On UNIX: `<WL_HOME>/server/lib`

   On Windows: `<WL_HOME>\server\lib`

   Note: `WL_HOME` is the path to the `wlserver_10.3` directory under the directory where you have installed Oracle WebLogic Server 10.3.3 before installing Oracle Identity Manager.

7. At the command prompt, run the following command:

   <full path to the directory where java is installed>`/java -jar wljarbuilder.jar`

   This command generates a library, which is required by all WebLogic Server application clients.

8. Install Oracle Identity Management 11*g* Release 1 (11.1.1.3.0) suite containing Oracle Identity Manager (OIM) and Oracle Access Manager (OAM), 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).

   For more information, see Important Notes Before You Begin.

9. Configure Oracle Identity Manager (OIM) and Oracle Access Manager (OAM) in a new or existing WebLogic administration domain, as described in OIM with LDAP Sync, and OAM. Note that Oracle Identity Manager and Oracle Access Manager must be in the same WebLogic domain. By default, this domain is located in the `<MW_HOME>\user_projects\domains` directory (on Windows). On UNIX, the domain is created in the `<MW_HOME>/user_projects/domains` directory. The path to this domain directory is referred to as *DOMAIN_HOME* in this chapter.

   However, do not set up LDAP Sync for Oracle Identity Manager at this stage. In addition, do not run the Oracle Identity Manager Configuration Wizard to configure Oracle Identity Manager Server at this stage.

21.5 Introduction to WebLogic Server Domain Agent

The WebLogic Server Domain Agent, referred to as Domain Agent in this chapter, provides out-of-the-box access protection for applications deployed in a WebLogic administration domain. This agent is enabled, by default. The agent is suitable for Oracle Identity Management environments where access protection of external applications or partners is not necessary.

The out-of-the-box agent provides the following features for applications deployed in a WebLogic domain:

- Authentication policy enforcement
- Authorization policy enforcement
- Front-channel authentication
- Identity assertion
- Back-channel anonymous authentication
- Session validation
- Logout

21.6 Setting Up Integration Between OIM and OAM Using the Domain Agent

After completing the prerequisites, you can set up integration between Oracle Identity Manager (OIM) and Oracle Access Manager (OAM) as follows:

1. Ensure that all the prerequisites, listed in Prerequisites, are satisfied. In addition, see Important Notes Before You Begin.
2. Ensure that the *WL_HOME* environment variable is set to the `wlserver_10.3` directory under your Middleware Home. On UNIX, it is the `<MW_HOME>/wlserver_10.3` directory. On Windows, it is the `<MW_HOME>\wlserver_10.3` directory. In addition, set the *JAVA_HOME* environment variable to the directory where the JDK is installed on your machine.
3. Open the `ldapconfig.props` file in a text editor. This file is located in the `server/ldap_config_util` directory under Oracle_IDM2, which is your IDM_Home for Oracle Identity Manager and Oracle Access Manager.
4. In the `ldapconfig.props` file, set values for the following parameters:
   - **OIMProviderURL** - Specify the URL for the OIM provider in the format: `t3://localhost:8003`
   - **OIDURL** - Specify the URL for the OID instance.
   - **OIDAdminUsername** - Specify the OID Administrator's user name, such as `cn=orcladmin`.
   - **OIDSearchBase** - Specify the OID search base, such as `ou=people,dc=com`.
   - **UserContainerName** - Specify the name of the user container, which is used as a default container of roles in the LDAP directory. For example, `cn=Users` and `cn=Groups`.
   - **RoleContainerName** - Specify the name of the user container, which is used as a default container of users in the LDAP directory.
   - **ReservationContainerName** - Specify the name of the user reservation container, which is used to reserve users while waiting for user creation approvals in Oracle Identity Manager. When the user creation is approved, users are moved from the reservation container to the actual user container.
5. On the command line, run the LDAP configuration pre-setup script (`LDAPConfigPreSetup.bat` on Windows, and `LDAPConfigPreSetup.sh` on UNIX). The files are located in the same `server/ldap_config_util` directory under your IDM_Home for Oracle Identity Manager and Oracle Access Manager.
6. When prompted, enter the OID administrator's password and the OIM administrator's password.

   Tip: After executing the `LDAPConfigPreSetup` script, you can run the following `ldapsearch` commands on the command line to verify that the necessary schema is created in Oracle Internet Directory:

   ```
   ldapsearch -p <OIDPORT> -D cn=orcladmin -w
   <ORCLADMIN_PASSWORD> -h <OIDHOST> -b
   "cn=subschemasubentry" -s base "objectclass=*"
   attributetypes | grep ob
   ```

   ```
   ldapsearch -p <OIDPORT> -D cn=orcladmin -w
   <ORCLADMIN_PASSWORD> -h <OIDHOST> -b
   "cn=subschemasubentry" -s base "objectclass=*"
   objectclasses | grep OIM
   ```

   The above `ldapsearch` commands should return rows if the `LDAPConfigPreSetup` script was successfully executed.

7. Configure Oracle Virtual Directory using Oracle Directory Services Manager to add adapters for users and changelog, as described in Task 2: Configuring OVD and OID for OIM.

> **Note:** Note that the `oamEnabled` parameter should be set to `true` if you are setting up integration between Oracle Identity Manager and Oracle Access Manager. You must do this when you configure the adapters.

8. Start the WebLogic Administration Server in the domain that manages Oracle Identity Manager and Oracle Access Manager. For information about starting the Administration Server, see Starting the Stack.

9. Update the Single Sign-On (SSO) provider configuration as follows:

   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 example IDM_Home directory for Oracle Identity Manager and Oracle Access Manager. For more information, see Important Notes Before You Begin.

   b. Use the WebLogic Scripting Tool (WLST) interface to add Oracle Access Manager Single Sign-On service instance and required properties 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 `addOAMSSOProvider` WLST Online command that adds an OAM SSO provider.

      ```
      addOAMSSOProvider(loginuri="/${app.context}/adfAuthentication", logouturi="/oamsso/logout.html", autologinuri="/obrar.cgi")
      ```

Table 21–2 WLST addOAMSSOProvider Command Arguments

Argument	Description
`loginuri`	Specifies the URI of the login page. Required.
`logouturi`	Specifies the URI of the logout page. Optional. If unspecified, defaults to logouturi=NONE. Set to "" to ensure that ADF security calls the OPSS logout service, which uses the implementation of the class OAMSSOServiceImpl to clear the cookie ObSSOCookie.
`autologinuri`	Specifies the URI of the autologin page. Optional. If unspecified, it defaults to autologin=NONE.

Tip: To verify the configuration the Single Sign-On (SSO) provider, complete the following steps:

1. From your present working directory, move to the following directory:

   `<DOMAIN_HOME>/config/fmwconfig`

2. Open the `jps-config.xml` file in a text editor.
3. In this file, you should see the following sets of entries, in addition to the existing entries:

```
<propertySet name="props.auth.uri.0">
            <property value="/oamsso/logout.html"
name="logout.url"/>
            <property value="/obrar.cgi"
name="autologin.url"/>
            <property
value="/$(app.context}/adfAuthentication"
name="login.url.BASIC"/>
            <property
value="/$(app.context}/adfAuthentication"
name="login.url.ANONYMOUS"/>
            <property
value="/$(app.context}/adfAuthentication"
name="login.url.FORM"/>
</propertySet>

<serviceInstance provider="sso.provider.0" name="sso.inst.0">

   1. <property
value="oracle.security.wls.oam.providers.sso.OAMSSOServiceProvi
derImpl" name="sso.provider.class"/>
```

c. Restart all Managed Servers and the WebLogic Administration Server in the domain. For more information about stopping the servers, see Stopping the Stack. For information about starting the servers, see Starting the Stack.

Note: If you have more than one host in the Oracle Identity Management domain, you must update the default value of the primaryAccessServer configuration parameter of the Domain Agent to the actual values.

---

10. Log in to My Oracle Support website (`http://support.oracle.com`), and search for the Single Sign-On Server **Patch 9824531**. Install this patch, as described in the readme file that is included in the patch.
11. Rewire Oracle Access Manager (OAM) to Oracle Internet Directory (OID) by running the `createUserIdentityStore` WLST command:

    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 example IDM_Home directory for Oracle Identity Manager and Oracle Access Manager. For more information, see Important Notes Before You Begin.

    Use the WebLogic Scripting Tool (WLST) interface to add Oracle Access Manager Single Sign-On service instance and required properties 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 Online command to configure Oracle Access Manager to use Oracle Internet Directory as its LDAP provider, as in the following example:

```
createUserIdentityStore(name="OAMOIDIdStoreForOIM",principal=
"cn=orcladmin", credential="testing1", 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.

If `orcladmin` is specified as `roleSecAdmin`, you may encounter permission problems when you run the RREG tool to register the Oracle HTTP Server 10*g* Webgate agent instead of the Domain Agent. Therefore, you must provide an appropriate group in Oracle Internet Directory user identity store in order to be able to run RREG to register the Oracle HTTP Server 10*g* Webgate agent.

You can also 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*.

Tip: To verify whether Oracle Access Manager is using Oracle Internet Directory as its LDAP provider, complete the following steps:

1. Open the `oam-config.xml` file in a text editor to verify whether the file contains an entry with the name specified in the `createUserIdentityStore` WLST command. The XML file is located in the `<DOMAIN_HOME>/config/fmwconfig` directory.
2. If this entry is present, verify whether value of the property `IsPrimary` for this entry is set to `true`.

12. Set up an OID authenticator as follows:

a. Log in to the Oracle WebLogic Administration Console.

b. In the **Domain Structure** section on the left navigation pane, click **Security Realms**. The Summary of Security Realms page is displayed.

c. In the **Change Center** section on the left navigation pane, click **Lock & Edit**.

d. On this page, click a default realm, such as `myrealm`. The Settings for myrealm page is displayed.

e. On this page, click the **Providers** tab.

f. Under **Authentication Providers**, click **New**. The Create a New Authentication Provider page is displayed.

g. On this page, enter a name for the provider in the **Name** text box. For example, `test`.

h. Select **OracleInternetDirectoryAuthenticator** from the **Type** drop-down list.

i. Click **OK**. The new provider `test` is listed on the Settings for myrealms page.

j. On this page, click the newly created authentication provider. The Settings for test page is displayed.

k. On this page, select **SUFFICIENT** as the **Control Flag**. Click **Save** to save the settings.

l. Exit the Oracle WebLogic Administration Console.

13. Configure Oracle Access Manager (OAM) for Oracle Identity Manager (OIM) integration as follows:

    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 example IDM_Home directory for Oracle Identity Manager and Oracle Access Manager. For more information, see Important Notes Before You Begin.

    Use the WebLogic Scripting Tool (WLST) interface to add Oracle Access Manager Single Sign-On service instance and required properties 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 `configureOIM` WLST Online command to configure Oracle Access Manager for OIM integration.

    ```
    configureOIM(oimHost = "<OIM_Host>" , oimPort = "<OIM_Port>",
    oimSecureProtocolEnabled = "false", oimAccessGatePwd =
    "<Password>", oimCookieDomain = "<cookie_domain>")
    ```

    `"<OIM_Host>"` and `"<OIM_Port>"` parameters in this WLST command refer to the Oracle Identity Manager Managed Server of Oracle Identity Manager when you are using the Oracle Identity Management domain agent and a single Oracle Identity Manager instance OIM. If you set secureProtocol to false, HTTP is used. If you set it to true, HTTPS is used.

Note: When you run the Oracle Identity Manager Configuration Wizard to configure Oracle Identity Manager Server at a later stage, you are required to enter values for **Password for Access Gate** and **Domain of Cookie** fields on the LDAP Sync and OAM screen in the configuration wizard. You must specify the same `oimAccessGatePwd` password and `oimCookieDomain` values.

Similarly, if you wish to use Oracle HTTP Server 10*g* Webgate for Oracle Access Manager instead of Domain Agent, you must specify the Webgate access password and cookie domain values for `oimAccessGatePwd` and `oimCookieDomain` parameters of the `configureOIM` command. In addition, you must specify the same values for **Password for Access Gate** and **Domain of Cookie** fields on the LDAP Sync and OAM screen in the Oracle Identity Manager Configuration Wizard.

For more information, see the LDAP Sync and OAM in the appendix Oracle Identity Manager Configuration Screens that contains descriptions of each screen in the Oracle Identity Manager Configuration Wizard.

Tip: To verify the configuration of Oracle Access Manager for OIM integration, complete the following steps:

1. Open the `oam-config.xml` file in a text editor to verify whether the file contains the agent profile entry `IdentityManagerAccessGate`. The XML file is located in the `<DOMAIN_HOME>/config/fmwconfig` directory.
2. In the same file, verify whether the OIM Port is listed in the IdentityManagement/ServerConfiguration section.

14. Run the Oracle Identity Manager Configuration Wizard to configure Oracle Identity Manager Server. To start the wizard, go to the `bin` directory under Oracle_IDM2 (your IDM_ORACLE_HOME for Oracle Identity Manager and Oracle Access Manager) and run the following command on the command line:

    - On Windows:

      ```
      config.bat
      ```

    - On UNIX:

      ```
      ./config.sh
      ```

15. Use the Oracle Identity Manager Configuration Wizard to configure Oracle Identity Manager, as described in Configuring OIM Server. While configuring Oracle Identity Manager Server, ensure that you select the **Enable Identity Administration Integration with OAM** option on the LDAP Sync and OAM screen.

    Note that you must enter the same values `oimAccessGatePwd` password and `oimCookieDomain`, specified in the `configureOIM WLST` command, as input to fields **Password of Access Gate** and **Domain of Cookie** on the LDAP Sync and OAM screen.

    When you choose to enable Identity Administration Integration with OAM using the Oracle Identity Manager Configuration Wizard, the **Enable LDAP Sync** option for OIM is selected, by default.

Proceed to complete the configuration of Oracle Identity Manager Server. When prompted, enter the OIM administrator's password and the `xelsysadm` password.

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

1. Check authenticator configuration as follows:

   1) Restart the WebLogic Administration Server. Log in to the WebLogic Server Administration Console.

   2) Click **Security Realms** > **myrealm** > **Providers**.

   3) Verify whether OAM Identity Asserter and OID Authenticator are listed. In addition, click the **Users and Groups** tab. Verify if OID users are populated.

2. Download the `oim-config.xml` file and verify the Single Sign-On (SSO) configuration information as follows:

   1) Start the Oracle Identity Manager Managed Server.

   2) Log in to Oracle Enterprise Manager Fusion Middleware ControlOracle Enterprise Manager Fusion Middleware Control using your WebLogic Server administrator credentials.

   3) Click **Identity and access** > **oim** > **oim(version)**. Right-click and select **System MBean Browser**. The System MBean Browser page is displayed.

   4) Under Application Defined MBeans, select `oracle.iam > Server:oim_server1 > Application: oim > XMLConfig > XMLConfig.SSOConfig > SSOConfig`.

   OAM's access server information used in OIM is displayed. Validate and verify the information.

16. Shut down the WebLogic Administration Server, as described in Stopping the Stack.
17. Log in to My Oracle Support website (`http://support.oracle.com`), and search for the Single Sign-On Server **Patch 9449855**. Install this patch, as described in the readme file that is included in the patch.
18. Restart the Administration Server and the Managed Servers (OIM, SOA, and OAM). For information about stopping the servers and then starting the servers, see Stopping the Stack and Starting the Stack.
19. On the command line, run the LDAP configuration post-setup script (`LDAPConfigPostSetup.bat` on Windows, and `LDAPConfigPostSetup.sh` on UNIX). The files are located in the `server/ldap_config_util` directory under your IDM_Home (**Oracle_IDM2**) for Oracle Identity Manager and Oracle Access Manager.

The integration between Oracle Identity Manager and Oracle Access Manager using the out-of-the-box Domain Agent is now complete.

21.7 Verifying the Configuration

After completing the configuration, you can verify the integration between Oracle Identity Manager and Oracle Access Manager as follows:

1. Access the Oracle Access Manager Administration Console (`http://<admin server host>:<admin server port>/oamconsole`).

   You should be redirected to Oracle Access Manager runtime environment. When you log in as a valid administrator, you must be able to access the console. The credential collector URL should be the URL of the Oracle Access Manager Managed Server. This page should contain links to **Forgot Password**, **Self Register**, and **Track Registration**.

2. Access the Oracle Identity Manager administration page (`http://<Host>:<OIM_Port>/admin/faces/pages/Admin.jspx`).

   The Oracle Access Manager login page from the Oracle Access Manager Managed Server should be displayed. This page should contain links to **Forgot Password**, **Self Register**, and **Track Registration**.

3. Log in as `xelsysadm`.

   You should be able to access the Oracle Identity Manager administration page.

4. Create a new user in the Oracle Identity Manager administration page.

   Log off the Oracle Identity Manager administration page and try to log in again using the newly created user name. When you provide valid credentials, you are prompted to reset the password and to set answers to challenge questions during first login. After this successful operation, you are redirected to the requested resource.

21.8 Using Oracle HTTP Server 10*g* Webgate for Oracle Access Manager 11*g*

If you wish to use Oracle HTTP Server 10*g* Webgate for Oracle Access Manager to protect the applications, the ones previously protected by the Domain Agent, you must migrate from the Domain Agent to Oracle HTTP Server 10*g* Webgate for Oracle Access Manager, as described in the chapter Migrating from Domain Agent to Oracle HTTP Server 10g Webgate for OAM.

22

Migrating from Domain Agent to Oracle HTTP Server 10*g* Webgate for OAM

This chapter describes how to migrate from the Domain Agent to Oracle HTTP Server 10*g* Webgate for Oracle Access Manager (OAM) to protect applications by using the same policy domain used by the Domain Agent. By default, applications deployed in an Oracle Identity Management 11.1.1.3.0 domain are protected by the Domain Agent.

> **Note:** Read this chapter only if you want to use Oracle HTTP Server 10*g* Webgate for Oracle Access Manager after setting up integration between Oracle Identity Manager and Oracle Access Manager, as described in the chapter Integration Between OIM and OAM.

This chapter discusses the following topics:

- Installing and Configuring Oracle HTTP Server 11g (11.1.1.3.0)
- Provisioning Oracle HTTP Server 10g Webgate for OAM Profile
- Installing Oracle HTTP Server 10g Webgate for OAM
- Configuring mod_weblogic
- Optional: Configuring Host Identifier
- Updating OIM Server Configuration
- Optional: Disabling Domain Agent
- Optional: Updating Oracle Identity Manager Configuration

22.1 Installing and Configuring Oracle HTTP Server 11*g* (11.1.1.3.0)

If you do not have an existing Oracle HTTP Server 11g (11.1.1.3.0) installation, you can install Oracle HTTP Server 11.1.1.2.0 and patch it to the latest version 11.1.1.3.0.

Oracle HTTP Server 11.1.1.2.0 is included in the Oracle Web Tier 11*g* Installer, you must download the Oracle Web Tier 11*g* (11.1.1.2.0) Installer from the Oracle Technology Network (OTN):

```
http://www.oracle.com/technology/software/products/middleware/htdocs/fmw_11_
download.html
```

Alternatively, you can download the latest Oracle Fusion Middleware 11*g* software from the following website:

```
http://edelivery.oracle.com/
```

Note: For information about installing and configuring Oracle HTTP Server 11*g* (11.1.1.2.0), see the "Installing Oracle Web Tier" topic in the *Oracle Fusion Middleware Installation Guide for Oracle Web Tier*. For information about patching Oracle HTTP Server 11.1.1.2.0 to 11.1.1.3.0 using the Patch Set Installer, see the "Applying the Latest Oracle Fusion Middleware Patch Set" topic in the *Oracle Fusion Middleware Patching Guide*.

After you install and configure Oracle HTTP Server, a working instance of Oracle HTTP Server is configured in an Instance Home.

22.2 Provisioning Oracle HTTP Server 10*g* Webgate for OAM Profile

For information about provisioning a profile for Oracle HTTP Server 10g Webgate for use with Oracle Access Manager 11*g* server, see the "Provisioning a 10g WebGate for Use with OAM 11g" topic in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager*.

Note: Ensure that the **hostIdentifier** parameter is set to `IDMDomain` and the **autoCreatePolicy** parameter is set to `false` when you are provisioning Oracle HTTP Server 10*g* Webgate to replace Domain Agent for OAM-OIM integration.

22.3 Installing Oracle HTTP Server 10*g* Webgate for OAM

For information about installing Oracle HTTP Server 10*g* Webgate for Oracle Access Manager (OAM), see the "Locating and Installing the Latest OAM 10g WebGate for OAM 11g" topic in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager*.

22.4 Configuring mod_weblogic

After installing Oracle HTTP Server 10*g* Webgate for Oracle Access Manager, you must configure the Web server to forward requests to the applications deployed on the WebLogic Server.

Open the `mod_wl_ohs.conf`, which is located in `<OHS_Instance_Home>/config/OHS/<Instance_Name>`, in a text editor and add appropriate entries, as in the following example:

```
<IfModule weblogic_module>
     <Location /oamconsole>
     SetHandler weblogic-handler
     WebLogicHost examplehost.exampledomain.com
     WebLogicPort   6162
     </Location>
     <Location /apmconsole>
     SetHandler weblogic-handler
     WebLogicHost examplehost.exampledomain.com
     WebLogicPort   6162
     </Location>
</IfModule>
```

Add similar Location entries for all the URIs for all the applications that were previously accessed directly on WebLogic Server.

After making the changes, restart Oracle HTTP Server. You can use the OPMN command-line tool to start or stop your Oracle HTTP Server instance. If any instances are running, run the following command on the command-line to stop all running instances:

```
<Oracle_Home_for_Oracle_HTTP_Server>/opmn/bin/opmnctl stopall
```

To restart the Oracle HTTP Server instance, run the following commands on the command line:

1. `<Oracle_Home_for_Oracle_HTTP_Server>/opmn/bin/opmnctl start`
2. `<Oracle_Home_for_Oracle_HTTP_Server>/opmn/bin/opmnctl startproc ias-component=<Oracle_HTTP_Server_Instance_Name>`

22.5 Optional: Configuring Host Identifier

This task is required only if you have set up integration between Oracle Identity Manager and Oracle Access Manager.

To configure host identifiers for auto-login functionality, complete the following steps:

1. Launch the Oracle Access Manager Administration Console (`http://<oamserverhost>:<adminport>/oamconsole`).
2. Click the **Policy Configuration** tab.
3. On the left navigation pane, click **Host Identifiers** > **IDMDomain**. The Host Identifier page is displayed.
4. In the **Operations** section on the Host Identifier page, all the host name and port number combinations are listed. Verify whether the section includes the host name and port number of the web server on which the Oracle HTTP Server 10*g* Webgate is configured.

   If it is not listed, add an entry as follows:

   a. On the **Operation** section, click the **+** icon. A new blank row is added to the Operations section.

   b. In the **Host Name** field, enter the host name of the web server on which the Oracle HTTP Server 10*g* Webgate is configured.

   c. In the **Port** field, enter the port number.

   d. Click **Apply**.

22.6 Updating OIM Server Configuration

Update the Oracle Identity Manager (OIM) configuration in the `oam-config.xml` file (located in the `<DOMAIN_HOME>/config/fmwconfig` directory) to ensure that the Host and Port attributes of the IdentityManagement element in the file point to the Oracle HTTP Server on which the Oracle HTTP Server Webgate 10*g* is configured:

1. Open the `oam-config.xml` file in a text editor.
2. Update the entries as follows:

```
<Setting Name="IdentityManagement" Type="htf:map">
      <Setting Name="ServerConfiguration" Type="htf:map">
      <Setting Name="OIM-SERVER-1" Type="htf:map">
```

```
      <Setting Name="Host" Type="xsd:string">OHS-HOST</Setting>
      <Setting Name="Port" Type="xsd:integer">OHS-PORT</Setting>
      <Setting Name="SecureMode" Type="xsd:boolean">false</Setting>
      </Setting>
</Setting>
```

Note: Ensure that you have set up integration between Oracle Identity Manager and Oracle Access Manager, as described in the topic "Integration Between OIM and OAM" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

After updating OIM Server configuration, you must perform logout configuration as follows:

1. Copy the `logout.html` file from the `<IDM_ORACLE_HOME>/oam/server/oamsso` directory to the `<10gWebgateInstallation>/access/oamsso` directory.
2. Edit the `SERVER_LOGOUTURL` variable in the `logout.html` file to point to the host and port of the Oracle Access Manager Server. Follow the instructions in the `logout.html` file.
3. If the `http.conf` file of the web server includes the following entries, remove the entries from the `http.conf` file:

```
<LocationMatch "/oamsso/*">
     Satisfy any
     </LocationMatch>
```

22.7 Optional: Disabling Domain Agent

Domain Agent, which runs on the Administration Server and all Managed Servers in the Oracle Identity Management domain, automatically detects the existence of a Webgate in the request flow. You do not need to disable the Domain Agent. However, if you want to disable the out-of-the-box Domain Agent, you can complete the following steps:

1. From your present working directory, move to the `<MW_HOME>/user_projects/domains/<name_of_your_WebLogic_domain>` directory (On UNIX). On Windows, move to the `<MW_HOME>\user_projects\domains\<name_of_your_WebLogic_domain>` directory.
2. To disable the Domain Agent running on the Administration Server, start the WebLogic Administration Server on the command line as follows:

   On UNIX:

   ```
   ./startWebLogic.sh -DWLSAGENT_DISABLED=true
   ```

   On Windows:

   ```
   startWebLogic.cmd -DWLSAGENT_DISABLED=true
   ```

3. From your present working directory, move to the `<MW_HOME>/user_projects/domains/<name_of_your_WebLogic_domain>/bin` directory (On UNIX). On Windows, move to the `<MW_HOME>\user_projects\domains\<name_of_your_WebLogic_domain</bin` directory.
4. To disable the Domain Agent running on Managed Servers in the domain, start the Managed Servers on the command line as follows:

On UNIX:

```
./startManagedWebLogic.sh <name_of_your_Managed_Server>
-DWLSAGENT_DISABLED=true
```

On Windows:

```
startManagedWebLogic.cmd <name_of_your_Managed_Server>
-DWLSAGENT_DISABLED=true
```

22.8 Optional: Updating Oracle Identity Manager Configuration

You can update the `<OHS_Instance_Home>/config/OHS/<ohs_name>/mod_wl_ohs.conf` to front-end Oracle Identity Manager URLs with Oracle HTTP Server.

To do so, complete the following steps:

Open the `mod_wl_ohs.conf` file in a text editor and add appropriate entries, as in the following example:

```
<IfModule weblogic_module>
     WebLogicHost OIM_MANAGED_SERVER_HOST
     WebLogicPort OIM_MANAGED_SERVER_PORT
     MatchExpression /oim*
     MatchExpression /admin*
     MatchExpression /xlWebApp*
     MatchExpression /Nexaweb*
     MatchExpression /workflowservice*
     MatchExpression /callbackService*
     MatchExpression /SchedulerService-web*
     MatchExpression /iam-consoles-faces*
</IfModule>
```

Replace the values of `OIM_MANAGED_SERVER_HOST` and `OIM_MANAGED_SERVER_PORT` with the values of Oracle Identity Manager Managed Server's host and port.

After making the changes, restart Oracle HTTP Server. You can use the OPMN command-line tool to start or stop your Oracle HTTP Server instance. If any instances are running, run the following command on the command-line to stop all running instances:

```
<Oracle_Home_for_Oracle_HTTP_Server>/opmn/bin/opmnctl stopall
```

To restart the Oracle HTTP Server instance, run the following commands on the command line:

1. `<Oracle_Home_for_Oracle_HTTP_Server>/opmn/bin/opmnctl start`
2. `<Oracle_Home_for_Oracle_HTTP_Server>/opmn/bin/opmnctl startproc ias-component=<Oracle_HTTP_Server_Instance_Name>`

Updating the OIM Configuration When the OAM URL or Agent Profile Changes

You can update the Oracle Identity Manager configuration when the name of the agent profile is modified or the OAM URL is modified.

To update Oracle Identity Manager configuration, complete the following steps:

1. Export the `oim-config.xml` file from metadata by running `<IDM_ORACLE_HOME>/server/bin/weblogicExportMetadata.sh` (on UNIX), and export the file - `/db/oim-config.xml`. On Windows operating systems, you can use the `weblogicExportMetadata.bat` file located in the same directory.

2. Update the file to use Oracle HTTP Server 10g Webgate by updating following element under the <ssoConfig> tag:

   <webgateType>javaWebgate</webgateType> to
   <webgateType>ohsWebgate10g</webgateType>

3. Import oim-config.xml back to metadata by running <IDM_Home>/server/bin/weblogicImportMetadata.sh on UNIX. On Windows, use the weblogicImportMetadata.bat located in the same directory.

4. Log in to Oracle Enterprise Manager Fusion Middleware Control using your WebLogic Server administrator credentials.

5. Click **Identity and access** > **oim** > **oim(version)**. Right-click and select **System MBean Browser**. The System MBean Browser page is displayed.

6. Under Application Defined MBeans, select oracle.iam > Server:oim_server1 > Application: oim > XMLConfig > config.

7. Replace the front-end URL with the URL of Oracle HTTP Server. This should be the same Oracle HTTP Server that was used before installing Oracle HTTP Server 10*g* Webgate for Oracle Access Manager. Complete the following steps:

   a. Under XMLConfig MBean, move to XMLConfig.DiscoveryConfig.

   b. Update **OimFrontEndURL** with the URL of Oracle HTTP Server.

   c. Click **Apply**.

8. Restart the OIM server.

23

Installing and Configuring Oracle HTTP Server 11*g* Webgate for OAM

This chapter describes how to install and configure Oracle HTTP Server 11*g* Webgate for Oracle Access Manager.

It discusses the following topics:

- Installation Overview
- Preparing to Install Oracle HTTP Server 11g Webgate for Oracle Access Manager
- Installing Oracle HTTP Server 11g Webgate for Oracle Access Manager
- Post-Installation Steps
- Verifying the Oracle HTTP Server 11g Webgate for Oracle Access Manager
- Getting Started with a New Oracle HTTP Server 11g Webgate Agent for Oracle Access Manager

> **Note:** Oracle HTTP Server 11*g* Webgate for Oracle Access Manager is not intended for use in Oracle Identity Management environments where you want to set up integration among Oracle Identity Management components.

23.1 Installation Overview

Installing Oracle HTTP Server 11*g* Webgate for Oracle Access Manager involves the following steps:

1. Installing Oracle HTTP Server 11.1.1.2.0, which is included in the Oracle Web Tier 11.1.1.2.0 Installer

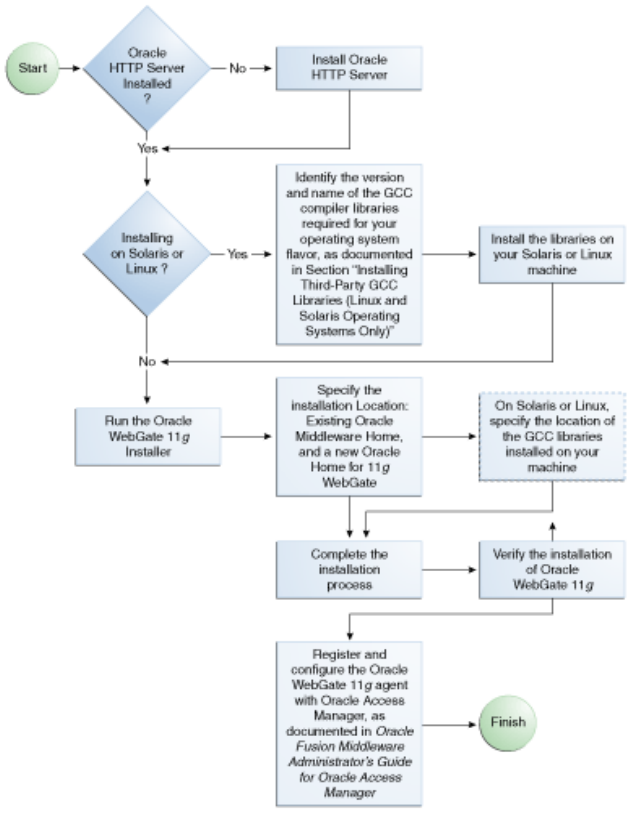
   > **Note:** If you have an existing Oracle HTTP Server 11.1.1.3.0 installation, which you patched from Oracle HTTP Server 11.1.1.2.0, you can use the same Oracle HTTP Server 11.1.1.3.0 installation.
   >
   > Oracle HTTP Server 11*g* Webgate for Oracle Access Manager requires either Oracle HTTP Server 11.1.1.2.0 or Oracle HTTP Server 11.1.1.3.0.

2. On Linux and Solaris operating systems: Installing third-party GCC libraries
3. Running the Oracle HTTP Server Webgate Installer to install Oracle HTTP Server 11*g* Webgate for Oracle Access Manager

4. Verifying the installation of Oracle HTTP Server 11*g* Webgate for Oracle Access Manager
5. Completing post-installation configuration steps
6. Registering the new Webgate agent

The following figure illustrates the process of installing Oracle HTTP Server 11*g* Webgate for Oracle Access Manager.

Figure 23–1 Oracle HTTP Server 11g Webgate Installation Process



As a standard practice, complete the following prerequisites for installing Oracle Fusion Middleware software:

1. Review Oracle Fusion Middleware certification information.

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

2. Review the system requirements.
3. Satisfy all dependencies, such as installing Oracle HTTP Server, which is included in the Oracle Web Tier Installer.
4. Perform the installation procedure for the appropriate component.
5. Verify the installation.

Table 23–1 lists the Installers and tools used to install and configure Oracle HTTP Server 11*g* Webgate for Oracle Access Manager at different stages of the installation and configuration process.

Table 23–1 Installation and Configuration Tools

Task	Tool
Install Oracle HTTP Server 11.1.1.2.0	Oracle Web Tier 11.1.1.2.0 Utilities Installer
Install Oracle HTTP Server Webgate 11*g*	Oracle HTTP Server Webgate 11*g* Installer
Register Webgate Agent	RREG Tool, or the Oracle Access Manager Administration Console
Start or Stop Process Instances	OPMN Command-Line Tool

23.2 Preparing to Install Oracle HTTP Server 11*g* Webgate for Oracle Access Manager

Oracle HTTP Server 11*g* Webgate for Oracle Access Manager requires Oracle HTTP Server 11*g* (11.1.1.2.0 or 11.1.1.3.0), which is included in the Oracle Web Tier 11*g* Installer.

You must run the Oracle Web Tier 11*g* Installer to install Oracle HTTP Server 11.1.1.2.0 and create an Oracle Home for Oracle Web Tier under a Middleware Home. If you have an existing Oracle HTTP Server 11.1.1.3.0 installation, which you patched from Oracle HTTP Server 11.1.1.2.0, you can use the same Oracle HTTP Server 11.1.1.3.0 installation.

In addition, if you are using the Linux or Solaris operating system, you must install third-party GCC libraries on your machine before installing Oracle HTTP Server 11*g* Webgate for Oracle Access Manager.

This section discusses the following topics:

- Oracle Fusion Middleware Certification
- Installing and Configuring OAM 11g
- Installing and Configuring Oracle HTTP Server 11g (11.1.1.2.0 or 11.1.1.3.0)
- Installing Third-Party GCC Libraries (Linux and Solaris Operating Systems Only)
- Prerequisites for 64-Bit Oracle HTTP Server 11g Webgates on Windows 2003 and Windows 2008 64-Bit Platforms

23.2.1 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/fusion-certification-100350.html`

23.2.2 Installing and Configuring OAM 11*g*

For information about installing Oracle Access Manager (OAM), see Installing OIM, OAM, OAAM, OAPM, and OIN (11.1.1.3.0). For information about configuring Oracle

Access Manager in a new or existing WebLogic administration domain, see Configuring Oracle Access Manager.

In addition, see the "Securing Communication Between OAM 11g Servers and WebGates" topic in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager* for information about configuring Oracle Access Manager in Open, Simple, or Cert mode.

23.2.3 Installing and Configuring Oracle HTTP Server 11*g* (11.1.1.2.0 or 11.1.1.3.0)

Oracle HTTP Server 11*g* Webgate for Oracle Access Manager is supported on both Oracle HTTP Server 11.1.1.2.0 and Oracle HTTP Server 11.1.1.3.0. Therefore, if you have an existing Oracle HTTP Server 11.1.1.3.0 installation, you do not need to install or patch any new version of Oracle HTTP Server.

If you wish to install Oracle HTTP Server 11.1.1.2.0, which is included in the Oracle Web Tier 11*g* Installer, you must download the Oracle Web Tier 11*g* (11.1.1.2.0) Installer from the Oracle Technology Network (OTN):

`http://www.oracle.com/technology/software/products/middleware/htdocs/fmw_11_download.html`

Alternatively, you can download the latest Oracle Fusion Middleware 11*g* software from the following website:

`http://edelivery.oracle.com/`

Note: For information about installing and configuring Oracle HTTP Server 11*g* (11.1.1.2.0), see the "Installing Oracle Web Tier" topic in the *Oracle Fusion Middleware Installation Guide for Oracle Web Tier*. For information about patching Oracle HTTP Server 11.1.1.2.0 to 11.1.1.3.0 using the Patch Set Installer, see the "Applying the Latest Oracle Fusion Middleware Patch Set" topic in the *Oracle Fusion Middleware Patching Guide*.

After you install and configure Oracle HTTP Server, a working instance of Oracle HTTP Server is configured in an Instance Home.

23.2.4 Installing Third-Party GCC Libraries (Linux and Solaris Operating Systems Only)

If you are installing Oracle HTTP Server 11*g* Webgate for Oracle Access Manager on a Linux or Solaris operating system, you must download and install third-party GCC libraries on your machine. See Table 23–2 for more information.

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

`http://gcc.gnu.org/`

Note: You must download sources from this website and compile them to obtain the GCC libraries.

For some operating systems, the required libraries may be available as installable packages from the support websites of operating system vendors.

Table 23–2 Versions of GCC Third-Party Libraries for Linux and Solaris

Operating System	Architecture	GCC Libraries	Required Library Version
Linux 32-bit	x86	libgcc_s.so.1 libstdc++.so.5	3.3.2
Linux 64-bit	x64	libgcc_s.so.1 libstdc++.so.6	3.4.6
Solaris 64-bit	SPARC	libgcc_s.so.1 libstdc++.so.5	3.3.2

23.2.5 Prerequisites for 64-Bit Oracle HTTP Server 11*g* Webgates on Windows 2003 and Windows 2008 64-Bit Platforms

If you are using Windows 2003 or Windows 2008 64-bit operating systems, you must install Microsoft Visual C++ 2005 libraries on the machine hosting the Oracle HTTP Server 11*g* Webgate for Oracle Access Manager.

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

`http://www.microsoft.com/DownLoads/details.aspx?familyid=EB4EBE2D-33C0-4A47-9DD4-B9A6D7BD44DA&displaylang=en`

23.3 Installing Oracle HTTP Server 11*g* Webgate for Oracle Access Manager

This section discusses the following topics:

- Launching the Installer
- Installation Flow and Procedure

23.3.1 Launching the Installer

The Installer program for Oracle HTTP Server 11*g* Webgate for Oracle Access Manager is included in the `webgate.zip` file.

Perform the following steps to start the installation wizard:

1. Extract the contents of the `webgate.zip` file to a directory. By default, this directory is named `webgate`.
2. Move to the `Disk1` directory under the `webgate` folder.
3. Start the Installer by executing one of the following commands:

   UNIX: `<full path to the runInstaller directory>./runInstaller -jreLoc <WebTier_Home>/jdk`

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

Note: When you install Oracle HTTP Server, the `jdk` directory is created under the `<WebTier_Home>` directory. You must enter the absolute path of the JRE folder located in this JDK when launching the installer. For example, on Windows, if the JDK is located in `D:\oracle\Oracle_WT1\jdk`, then launch the installer from the command prompt as follows:

```
D:\setup.exe -jreLoc D:\oracle\Oracle_WT1\jdk
```

After the Installer starts, the Welcome screen appears. Continue by referring to the section Installation Flow and Procedure for installing Oracle HTTP Server 11*g* Webgate for Oracle Access Manager.

23.3.2 Installation Flow and Procedure

Follow the instructions in Table 23–3 to install Oracle HTTP Server 11*g* Webgate for Oracle Access Manager.

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

Table 23–3 Installation Flow

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. Note that the Middleware Home should contain an Oracle Home for Oracle Web Tier. Oracle WebLogic Server is not a prerequisite for installing Oracle HTTP Server Webgate. However, Oracle HTTP Server, which is a component of Oracle Web Tier, requires only the directory structure for the Middleware home. 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	On selected UNIX operating systems only (Linux 32- and 64-bit, and Solaris 64-bit): Specify GCC Library Screen	Specify the directory that contains the GCC libraries. Click **Next** to continue.
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.

23.4 Post-Installation Steps

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

1. Move to the following directory under your Oracle Home for Webgate:

   On UNIX operating systems:

   ```
   <Webgate_Home>/webgate/ohs/tools/deployWebGate
   ```

   On Windows operating systems:

   ```
   <Webgate_Home>\webgate\ohs\tools\deployWebGate
   ```

2. On the command line, run the following command to copy the required bits of agent from the Webgate_Home directory to the Webgate Instance location:

   On UNIX operating systems:

   ```
   ./deployWebgateInstance.sh -w <Webgate_Instance_Directory>
   -oh <Webgate_Oracle_Home>
   ```

   On Windows operating systems:

   ```
   deployWebgateInstance.bat -w <Webgate_Instance_Directory> -oh
   <Webgate_Oracle_Home>
   ```

   Where `<Webgate_Oracle_Home>` is the directory where you have installed Oracle HTTP Server Webgate and created as the Oracle Home for Webgate, as in the following example:

   ```
   <MW_HOME>/Oracle_OAMWebGate1
   ```

   The `<Webgate_Instance_Directory>` is the location of Webgate Instance Home, which is same as the Instance Home of Oracle HTTP Server, as in the following example:

   ```
   <MW_HOME>/Oracle_WT1/instances/instance1/config/OHS/ohs1
   ```

   Note that an Instance Home for Oracle HTTP Server is created after you configure Oracle HTTP Server. This configuration is performed after installing Oracle HTTP Server 11.1.1.2.0 or patching to Oracle HTTP Server 11.1.1.3.0.

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

   On UNIX (depending on the shell):

   ```
   export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:<Oracle_Home_for_
   Oracle_HTTP_Server>/lib
   ```

   On Windows:

   Set the `<Webgate_Installation_Directory>\webgate\ohs\lib` location and the `<Oracle_Home_for_Oracle_HTTP_Server>\bin` location in the `PATH` environment variable. Add a semicolon (;) followed by this path at the end of the entry for the `PATH` environment variable.

4. From your present working directory, move up one directory level:

   On UNIX operating systems, move to:

   ```
   <Webgate_Home>/webgate/ohs/tools/setup/InstallTools
   ```

   On Windows operating systems, move to:

   ```
   <Webgate_Home>\webgate\ohs\tools\EditHttpConf
   ```

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

On UNIX operating systems:

```
./EditHttpConf -w <Webgate_Instance_Directory> [-oh <Webgate_
Oracle_Home>] [-o <output_file>]
```

On Windows operating systems:

```
EditHttpConf.exe -w <Webgate_Instance_Directory> [-oh
<Webgate_Oracle_Home>] [-o <output_file>]
```

Note: The `-oh <WebGate_Oracle_Home>` and `-o <output_file>` parameters are optional.

Where `<Webgate_Oracle_Home>` is the directory where you have installed Oracle HTTP Server Webgate for Oracle Access Manager and created as the Oracle Home for Webgate, as in the following example:

```
<MW_HOME>/Oracle_OAMWebGate1
```

The `<Webgate_Instance_Directory>` is the location of Webgate Instance Home, which is same as the Instance Home of Oracle HTTP Server, as in the following example:

```
<MW_HOME>/Oracle_WT1/instances/instance1/config/OHS/ohs1
```

The `<output_file>` is the name of the temporary output file used by the tool, as in the following example:

```
Edithttpconf.log
```

Note that an Instance Home for Oracle HTTP Server is created after you configure Oracle HTTP Server. This configuration is performed after installing Oracle HTTP Server 11.1.1.2.0 or patching to Oracle HTTP Server 11.1.1.3.0.

23.5 Verifying the Oracle HTTP Server 11*g* Webgate for Oracle Access Manager

After completing the installation of Oracle HTTP Server 11*g* Webgate for Oracle Access Manager, including the post-installation steps, you can examine the *`installDATE-TIME_STAMP.out`* log file to verify the installation.

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

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

23.6 Getting Started with a New Oracle HTTP Server 11*g* Webgate Agent for Oracle Access Manager

Before you can get started with the new Oracle HTTP Server 11*g* Webgate agent for Oracle Access Manager, you must complete the following tasks:

1. Register the New Webgate Agent
2. Copy Generated Files and Artifacts to the Webgate Instance Location
3. Restart the Oracle HTTP Server Instance

23.6.1 Register the New Webgate Agent

You can register the new Webgate agent with Oracle Access Manager by using the Oracle Access Manager Administration Console. For more information, see the "Registering Partners (Agents and Applications) by Using the Console" topic in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager*.

Alternatively, you can use the RREG command-line tool to register a new Webgate agent. The tool can be run in two modes: **In-Band** mode, and **Out-Of-Band** mode.

Setting Up the RREG Tool

1. After installing and configuring Oracle Access Manager, navigate to the following location:

   On UNIX operating systems:

   `<IDM_Home>/oam/server/rreg/client`

   On Windows operating systems:

   `<IDM_Home>\oam\server\rreg\client`

2. On the command line, untar the RREG.tar.gz file using `gunzip`, as in the following example:

   ```
   gunzip RREG.tar.gz
   tar -xvf RREG.tar
   ```

The tool used to register the agent is located in the following location:

On UNIX operating systems:

`<RREG_Home>/bin/oamreg.sh`

On Windows operating systems:

`<RREG_Home>\bin\oamreg.bat`

> **Note:** `<RREG_Home>` is the directory where you extracted the contents of `RREG.tar.gz/rreg` to.

Set the following environment variables in the `oamreg.sh` or `oamreg.bat` script:

- `OAM_REG_HOME` - Set this variable to the absolute path to the directory where you extracted the contents of `RREG.tar/rreg`.
- `JDK_HOME` - Set this variable to the absolute path to the directory where Java/JDK is installed on your machine.

Updating the OAM11gRequest.xml File

You must update the agent parameters, such as `agentName`, in the `OAM11GRequest.xml` file located in the `<RREG_Home>\input` directory on the Windows operating system. On the UNIX operating system, the file is located in the `<RREG_Home>/input` directory.

> **Note:** The `OAM11GRequest.xml` file or the short version `OAM11GRequest_short.xml` is used as a template. You can copy this template file and use.

In-Band Mode

If you run the RREG tool once after updating the Webgate parameters in the `OAM11GRequest.xml` file, the files and artifacts required by Webgate are generated in the following directory:

On UNIX operating systems:

```
<RREG_Home>/output/<agent_name>
```

On Windows operating systems:

```
<RREG_Home>\output\<agent_name>
```

> **Note:** You can run RREG either on a client machine or on the server machine. If you are running it on the server machine, you must manually copy the artifacts back to the client machine.

Complete the following steps:

1. Open the `OAM11GRequest.xml` file, which is located in the `input` directory (`<RREG_Home>/input/` on UNIX, and `<RREG_Home>\input` on Windows). `<RREG_Home>` is the directory where you extracted the contents of `RREG.tar.gz/rreg` to. Edit this XML file and fill in parameters for the new Oracle HTTP Server Webgate for Oracle Access Manager.
2. Run the following command on the command line:

   On UNIX operating systems:

   ```
   ./<RREG_Home>/bin/oamreg.sh inband input/OAM11GRequest.xml
   ```

   On Windows operating systems:

   ```
   <RREG_Home>\bin\oamreg.bat inband input\OAM11GRequest.xml
   ```

Out-Of-Band Mode

If you are an end-user with no access to the server, you can email your updated `OAM11GRequest.xml` file to the system administrator, who can run RREG in the Out-Of-Band mode. You can collect the generated `<AgentID>_Response.xml` file from the system administrator and run RREG on this file to obtain the Webgate files and artifacts you require.

After you receive the generated `<AgentID>_Response.xml` file from the administrator, you must manually copy the file to the `input` directory on your machine.

Complete the following steps:

1. If you are an end-user with no access to the server, open the `OAM11GRequest.xml` file, which is located in the `input` directory (`<RREG_Home/input/` on UNIX, and `<RREG_Home\input\` on Windows). `<RREG_Home>` is the directory where you extracted the contents of `RREG.tar.gz/rreg` to. Edit this XML file and fill in parameters for the new Oracle HTTP Server Webgate for Oracle Access Manager. Send the updated file to your system administrator.
2. If you are an administrator, copy the updated `OAM11GRequest.xml` file to the `input` directory on your machine (`<RREG_Home>/input/` on UNIX, and `<RREG_Home>\input\` on Windows). This is the file you received from the

end-user. Move to your (administrator's) RREG_Home directory and run the following command on the command line:

On UNIX operating systems:

```
./<RREG_Home>/bin/oamreg.sh outofband input/OAM11GRequest.xml
```

On Windows operating systems:

```
<RREG_Home>\bin\oamreg.bat outofband input\OAM11GRequest.xml
```

An `<Agent_ID>_Response.xml` file is generated in the `output` directory on the administrator's machine (`<RREG_Home>/output/` on UNIX, and `<RREG_Home>output\` on Windows). Send this file to the end-user who sent you the updated `OAM11GRequest.xml` file.

3. If you are an end-user, copy the generated `<Agent_ID>_Response.xml` file to your `input` directory (`<RREG_Home>/input/` on UNIX, and `<RREG_Home>input\` on Windows). This is the file you received from the administrator. Move to your (client's) RREG home directory and run the following command on the command line:

   On UNIX operating systems:

   ```
   ./<RREG_Home>/bin/oamreg.sh outofband input/<Agent_ID>_Response.xml
   ```

   On Windows operating systems:

   ```
   <RREG_Home>\bin\oamreg.bat outofband input\<Agent_ID>_Response.xml
   ```

   Note: If you register the Webgate agent using the Oracle Access Manager Administration Console, as described in the "Registering Partners (Agents and Applications) by Using the Console" topic in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager*, you must manually copy the files and artifacts generated after the registration from the server machine (the machine where Oracle Access Manager Administration Console is running) to the client machine. The files and artifacts are generated in the `<MW_HOME>/user_projects/domains/<name_of_the_WebLogic_domain_for_OAM>/output/<Agent_ID>` directory.

Files and Artifacts Generated by RREG

Regardless of the method or mode you use to register the new Webgate agent, the following files and artifacts are generated in the `<RREG_Home>/output/<Agent ID>` directory:

- `cwallet.sso`
- `ObAccessClient.xml`
- In the **SIMPLE** mode, RREG generates:
  - `password.xml`, which contains the obfuscated global passphrase to encrypt the private key used in SSL. This passphrase can be the same as the passphrase used on the server.
  - `aaa_key.pem`
  - `aaa_cert.pem`

- In the **CERT** mode, RREG generates:

  `password.xml`, which contains the obfuscated global passphrase to encrypt the private key used in SSL. This passphrase can be different than the passphrase used on the server.

> **Note:** You can use these files generated by RREG to generate a certificate request and to get it signed by a third-party Certification Authority. To install an existing certificate, you must use the existing `aaa_cert.pem` and `aaa_chain.pem` files along with `password.xml` and `aaa_key.pem`.

23.6.2 Copy Generated Files and Artifacts to the Webgate Instance Location

After RREG generates these files and artifacts, you must manually copy them (`cwallet.sso, ObAccessClient.xml, password.xml, aaa_key.pem, aaa_cert.pem`, based on the security mode you are using) from the `<RREG_Home>/output/<Agent ID>` directory to the `<Webgate_Instance_Home>` directory.

In **OPEN** mode, copy the following files from the `<RREG_Home>/output/<Agent_ID>` directory to the <Webgate_Instance_Home>/webgate/config directory:

- `ObAccessClient.xml`
- `cwallet.sso`

In **SIMPLE** mode, copy the following files from the `<RREG_Home>/output/<Agent_ID>` directory to the <Webgate_Instance_Home>/webgate/config directory:

- `ObAccessClient.xml`
- `cwallet.sso`
- `password.xml`

In addition, copy the following files from the `<RREG_Home>/output/<Agent_ID>` directory to the `<Webgate_Instance_Home>/webgate/config/simple` directory:

- `aaa_key.pem`
- `aaa_cert.pem`

In **CERT** mode, copy the following files from the `<RREG_Home>/output/<Agent_ID>` directory to the `<Webgate_Instance_Home>/webgate/config` directory:

- `ObAccessClient.xml`
- `cwallet.sso`
- `password.xml`

After copying the files, you must either generate a new certificate or migrate an existing certificate.

Generating a New Certificate

You can generate a new certificate as follows:

1. From your present working directory, move to the `<Webgate_Home>/webgate/ohs/tools/openssl` directory.

2. On the command line, create a certificate request as follows:

```
./openssl req -utf8 -new -nodes -config openssl_silent_
ohs11g.cnf -keyout aaa_key.pem -out aaa_req.pem -rand
<Webgate_Home>/webgate/ohs/config/random-seed
```

3. Self-sign the certificate as follows:

```
./openssl ca -config openssl_silent_ohs11g.cnf -policy
policy_anything -batch -out aaa_cert.pem -infiles aaa_req.pem
```

4. Copy the following generated certificates to the <Webgate_Instance_Home>/webgate/config directory:
   - aaa_key.pem
   - aaa_cert.pem
   - cacert.pem located in the simpleCA directory

> **Note:** After copying the cacert.pem file, you must rename the file to aaa_chain.pem.

Migrating an Existing Certificate

If you want to migrate an existing certificate (aaa_key.pem, aaa_cert.pem, and aaa_chain.pem), be sure to remember the passphrase that you used to encrypt aaa_key.pem. You must enter the same passphrase during the RREG registration process. If you do not use the same passphrase, the password.xml file generated by RREG does not match the paraphrase used to encrypt the key.

If you enter the same passphrase, you can copy these certificates as follows:

1. From your present working directory, move to the <Webgate_Instance_Home>/webgate/config directory.
2. Copy the following certificates to the <Webgate_Instance_Home>/webgate/config directory:
   - aaa_key.pem
   - aaa_cert.pem
   - aaa_chain.pem

23.6.3 Restart the Oracle HTTP Server Instance

You can use the Oracle Process Manager and Notification Server (OPMN) command-line tool to start or stop your Oracle HTTP Server instance. If any instances are running, run the following command on the command-line to stop all running instances:

```
<Oracle_Home_for_Oracle_HTTP_Server>/opmn/bin/opmnctl stopall
```

To restart the Oracle HTTP Server instance, run the following commands on the command line:

1. <Oracle_Home_for_Oracle_HTTP_Server>/opmn/bin/opmnctl start
2. <Oracle_Home_for_Oracle_HTTP_Server>/opmn/bin/opmnctl startproc ias-component=<Oracle_HTTP_Server_Instance_Name>

24

Lifecycle Management

This chapter explains how to address situations where a lifecycle change event occurs for an Oracle Identity Management component that is integrated with one or more components.

Topics include:

24.1 How Lifecycle Events Impact Integrated Components

Following are ways in which certain lifecycle events, sometimes referred to as rewiring, affect a component that is already integrated with others:

- Reassociation

  The hostname or port of an integrated component is reassociated. For example, the hostname of an OVD server changes.

- Test to Production

  When entities in a test or pilot environment are migrated into a pre-installed production environment, this can affect dependent components. For example, moving Oracle Identity Manager Navigator to a new production environment.

> **Note:** For some components, "rewiring" to achieve Test to Production is not feasible, and it is advisable to simply create a new production instance of the server. Oracle Identity Federation is an example of a server that is freshly installed in the production environment rather than changing the test configuration.

24.2 LCM for Oracle Identity Manager

Lifecycle management events for Oracle Identity Manager include:

- reassociation when the host or port changes for these components:
  - Oracle Virtual Directory

  - Oracle SOA Suite
  - MDS
- moving metadata from a test environment to a production environment

Refer to the following sources for lifecycle management procedures relating to OIM:

- "Oracle Virtual Directory Host and Port Changes" in the *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager*
- "Changing OVD Password" in the *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager*
- "SPML Client Host and Port Changes" in the *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager*
- "SOA Host and Port Changes" in the *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager*
- "Oracle Identity Manager Database Host and Port Changes" in the *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager*
- "Oracle Identity Manager (OIM) Rewiring with Existing Oracle Adaptive Access Manager (OAAM)" in the *Oracle Fusion Middleware Developer's Guide for Oracle Adaptive Access Manager*
- "Changing Oracle Identity Manager Database Password" in the *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager*
- "Configuring LDAP Adapters" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Virtual Directory*
- "Adding a Component Link to the Product Launcher by Using Product Discovery" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Navigator*
- "Editing Adapter Plug-Ins" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Virtual Directory*
- "Move Oracle Identity Manager to a New Production Environment" in the *Oracle Fusion Middleware Administrator's Guide*
- "Move Oracle Identity Manager to an Existing Production Environment" in the *Oracle Fusion Middleware Administrator's Guide*

24.3 LCM for Oracle Access Manager

Lifecycle events for Oracle Access Manager include replicating the policy configuration information from the test system into production.

Refer to the following sources for lifecycle management procedures relating to OAM:

- "Adding a Component Link to the Product Launcher by Using Product Discovery" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Navigator*
- "Moving OAM 11g Data from a Test to a Production Deployment" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager*

24.4 LCM for Oracle Adaptive Access Manager

Lifecycle events for Oracle Adaptive Access Manager include reassociation when the host or port changes for the following components:

- Oracle Virtual Directory

- Oracle Internet Directory
- Oracle Database
- Oracle Identity Manager

Refer to the following sources for lifecycle management procedures relating to OAAM:

- "Adding a Component Link to the Product Launcher by Using Product Discovery" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Navigator*
- "Oracle Virtual Directory (OVD) Rewiring with Existing Oracle Adaptive Access Manager (OAAM)" in the *Oracle Fusion Middleware Developer's Guide for Oracle Adaptive Access Manager*
- "Oracle Identity Manager (OIM) Rewiring with Existing Oracle Adaptive Access Manager (OAAM)" in the *Oracle Fusion Middleware Developer's Guide for Oracle Adaptive Access Manager*
- "OID Rewiring with Existing OAAM (in Cases without OVD)" in the *Oracle Fusion Middleware Developer's Guide for Oracle Adaptive Access Manager*
- "Database Rewiring with Existing OAAM" in the *Oracle Fusion Middleware Developer's Guide for Oracle Adaptive Access Manager*
- "Move Oracle Adaptive Access Manager to a New Production Environment" in the *Oracle Fusion Middleware Administrator's Guide*
- "Move Oracle Adaptive Access Manager to an Existing Production Environment" in the *Oracle Fusion Middleware Administrator's Guide*

24.5 LCM for Oracle Identity Navigator

Lifecycle events for Oracle Identity Navigator include migrating from test to production, and rewiring the integration with Oracle Business Intelligence Publisher.

Refer to the following sources for lifecycle management procedures relating to OIN:

- "Migrating Oracle Identity Navigator from Test to Production" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Navigator*.
- "Configuring Oracle Business Intelligence Publisher" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Navigator*.
- "Adding a Component Link to the Product Launcher by Using Product Discovery" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Navigator*
- "Migrating Oracle Identity Navigator from Test to Production" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Navigator*

24.6 References

For additional information about lifecycle management in Oracle Fusion Middleware, see "Part V Advanced Administration: Expanding Your Environment" in the *Oracle Fusion Middleware Administrator's Guide*.

Part IV

Appendixes

Part IV contains the following appendixes:

- Appendix B, "Starting or Stopping the Oracle Stack"
- Appendix C, "Performing Silent Installations"
- Appendix A, "Deinstalling and Reinstalling Oracle Identity Management"
- Appendix D, "Troubleshooting the Installation"
- Appendix E, "OAAM Partition Schema Reference"
- Appendix F, "Oracle Identity Management 11.1.1.3.0 Software Installation Screens"
- Appendix G, "WebLogic Domain Configuration Screens"
- Appendix H, "Oracle Identity Manager Configuration Screens"
- Appendix I, "Software Deinstallation Screens"

A

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. It 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 *IDM_ORACLE_HOME*`/oui/bin directory` (UNIX) or the *IDM_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.

Table A–1 (Cont.) Deinstallation Types

Type	Description
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.

  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. To know all the processes that are using *ORACLE_COMMON_HOME* directory use the following commands:

   On UNIX:

   ```
   ps-ef grep <oracle_common>
   ```

   On Windows:

   Use the Windows Task Manager to identify the processes that use the *ORACLE_COMMON_HOME* directory.

2. Deinstall your Oracle Identity Management Oracle Home by performing the steps in Deinstalling the Oracle Identity Management Oracle Home.

3. Open a command prompt and move (cd) into the *ORACLE_COMMON_HOME*/oui/bin/ directory (on UNIX) or the *ORACLE_COMMON_HOME*\oui\bin\ directory (on Windows).
4. Invoke the Deinstaller from command line using the -deinstall option and the -jreLoc option, which identifies the location where Java Runtime Environment (JRE) is installed. For example:

   On UNIX:

   ```
   ./runInstaller -deinstall -jreLoc FULL_PATH_TO_JRE_DIRECTORY
   ```

   On Windows:

   ```
   setup.exe -deinstall -jreLoc FULL_PATH_TO_JRE_DIRECTORY
   ```

   The Welcome screen appears.
5. Click **Next**. The Select Deinstallation Type screen appears.
6. Select the **Deinstall Oracle Home** option at the top of the Select Deinstallation Type screen.

   Note: The path to the *ORACLE_COMMON_HOME* directory appears in the text describing the **Deinstall Oracle Home** option.

   Click **Next**. The Deinstall Oracle Home screen appears.
7. Confirm the correct *ORACLE_COMMON_HOME* directory is listed and click **Deinstall**.

   The Deinstallation Progress screen appears, along with a Warning dialog box prompting you to confirm that you want to deinstall the *ORACLE_COMMON_HOME* directory.
8. Click **Yes** on the Warning dialog box to confirm you want to remove the *ORACLE_COMMON_HOME* directory. The deinstallation begins.
9. Click **Finish** after the deinstallation progresses to 100%. The Deinstallation Complete screen appears.
10. Click **Finish** on the Deinstallation Complete screen to exit the deinstaller.

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/technology/documentation/oim1014.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 11g Release1(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 or Stopping the Oracle Stack

You must start or stop the components of the Oracle stack in a specific order. This appendix describes that order and contains the following topics:

- Starting the Stack
- Stopping the Stack
- Restarting Servers

Note: When executing the startManagedWebLogic and stopManagedWebLogic scripts described in the following topics:

- *SERVER_NAME* represents the name of the Oracle WebLogic Managed Server, such as wls_oif1, wls_ods1, or oam_server1.
- You will be prompted for values for *USER_NAME* and *PASSWORD* if you do not provide them as options when you execute the script.
- The value for *ADMIN_URL* will be inherited if you do not provide it as an option when you execute the script.

B.1 Starting the Stack

After completing the installation and domain configuration, you must start the Administration Server and various Managed Servers to get your deployments up and running:

1. To start the Administration Server, run the `startWebLogic.sh` (on UNIX operating systems) or `startWebLogic.cmd` (on Windows operating systems) script in the directory where you created your new domain.

   On UNIX systems:

   MW_HOME`/user_projects/domains/`*domain_name*`/startWebLogic.sh`

   On Windows systems:

   MW_HOME`\user_projects\domains\`*domain_name*`\startWebLogic.cmd`

   You entered the domain name and location on the Specify Domain Name and Location Screen in the Configuration Wizard.

2. Ensure that the Node Manager is running. Oracle WebLogic Administration Server does not do this automatically. If the Node Manager is not running, start the Node Manager by executing the following command:

```
$WLS_HOME/server/bin/startNodeManager.sh
```

3. Start system components, such as Oracle Internet Directory and Oracle Virtual Directory, by executing the following command:

   ```
   ORACLE_INSTANCE/bin/opmnctl startall
   ```

   You can verify that the system components have started by executing the following command:

   ```
   ORACLE_INSTANCE/bin/opmnctl status -l
   ```

4. To start the Managed Servers, run the `startManagedWebLogic.sh` (on UNIX operating systems) or `startManagedWebLogic.cmd` (on Windows operating systems) script in the `bin` directory inside the directory where you created your domain. You must start these Managed Servers from the command line.

   This command also requires that you specify a server name. You must start the servers you created when configuring the domain, as shown in the following example:

   - `oam_server1` (Oracle Access Manager Server)
   - `oim_server1` (Oracle Identity Manager Server)

   For example, to start Oracle Access Manager Server on a UNIX system:

   ```
   MW_HOME/user_projects/domains/domain_name/bin/startManagedWebLogic.sh oam_
   server1
   ```

   On Windows systems:

   ```
   MW_HOME\user_projects\domains\domain_name\bin\startManagedWebLogic.cmd oam_
   server1
   ```

   Before the Managed Server is started, you are prompted for the WebLogic Server user name and password. These were provided on the Configure Administrator Username and Password Screen in the Configuration Wizard.

   If your Administration Server is using a non-default port, or resides on a different host than your Managed Servers (in a distributed environment), you must also specify the URL to access your Administration Server.

   On UNIX systems:

   ```
   MW_HOME/user_projects/domains/domain_name/bin/startManagedWebLogic.sh oam_
   server1 http://host:admin_server_port
   ```

   On Windows systems:

   ```
   MW_HOME\user_projects\domains\domain_name\bin\startManagedWebLogic.cmd oam_
   server1 http://host:admin_server_port
   ```

   Instead of being prompted for the Administration Server user name and password, you can also specify them directly from the command lime.

   On UNIX systems:

   ```
   MW_HOME/user_projects/domains/domain_name/bin/startManagedWebLogic.sh oam_
   server1 http://host:admin_server_port -Dweblogic.management.username=user_name
   -Dweblogic.management.password=password
   ```

   On Windows systems:

   ```
   MW_HOME\user_projects\domains\domain_name\bin\startManagedWebLogic.cmd oam_
   ```

```
server1 http://host:admin_server_port -Dweblogic.management.username=user_name
-Dweblogic.management.password=password
```

> **Note:** You can use the Oracle WebLogic Administration Console to start managed components in the background. See *Oracle Fusion Middleware Introduction to Oracle WebLogic Server* for more information.

If you do not know the names of the Managed Servers that should be started, you can view the contents of the following file on UNIX systems:

```
MW_HOME/user_projects/domains/domain_name/startManagedWebLogic_readme.txt
```

On Windows systems:

```
MW_HOME\user_projects\domains\domain_name\startManagedWebLogic_readme.txt
```

Or, you can access the Administration Server console at the following URL:

```
http://host:admin_server_port/console
```

Supply the user name and password that you specified on the Configure Administrator Username and Password Screen of the Configuration Wizard. Then, navigate to **Environment > Servers** to see the names of your Managed Servers.

B.2 Stopping the Stack

You can stop the Oracle WebLogic Administration Server and all the managed servers by using Oracle WebLogic Administration Console. See *Oracle Fusion Middleware Introduction to Oracle WebLogic Server* for more information.

To stop the stack components from the command line, perform the following steps:

1. Stop WebLogic managed components, such as Oracle Directory Integration Platform, Oracle Identity Federation, Oracle Directory Services Manager, Oracle Access Manager, Oracle Identity Manager, and Oracle Adaptive Access Manager, by executing the following command:

   ```
   MW_HOME/user_projects/domains/DOMAIN_NAME/bin/stopManagedWebLogic.sh \
   {SERVER_NAME} {ADMIN_URL} {USER_NAME} {PASSWORD}
   ```

2. Stop system components, such as Oracle Internet Directory and Oracle Virtual Directory, by executing the following command:

   ```
   ORACLE_INSTANCE/bin/opmnctl stopall
   ```

3. Stop the Oracle WebLogic Administration Server by executing the following command:

   ```
   MW_HOME/user_projects/domains/DOMAIN_NAME/bin/stopWebLogic.sh
   ```

4. If you want to stop the Node Manager, you can use the `kill` command:

   ```
   kill -9 PID
   ```

B.3 Restarting Servers

To restart the Administration Server or Managed Servers, you must stop the running Administration Server or Managed Servers first before starting them again. For more information, see Stopping the Stack and Starting the Stack.

C

Performing Silent Installations

This appendix describes how to install Oracle Identity Management in silent mode. This appendix contains the following topics:

C.1 What is a Silent Installation?

A silent installation eliminates the need to monitor the Oracle Identity Management installation because no graphical output is displayed and no input by the user is required.

To perform a silent Oracle Identity Management installation, you invoke the Installer with the -silent flag and provide a response file from the command line. The response file is a text file containing variables and parameter values which provide answers to the Installer prompts.

C.2 Before Performing a Silent Installation

This topic describes tasks that may be required before you perform a silent installation. This topic includes the following sections:

C.2.1 UNIX Systems: Creating the oraInst.loc File

The Installer uses the Oracle inventory directory to keep track of all Oracle products installed on the systems. The inventory directory is stored in a file named oraInst.loc. If this file does not already exist on your system, you must create it before starting a silent installation.

Perform the following steps to create the oraInst.loc file if it does not exist:

1. Log in as the root user.
2. Using a text editor such as vi or emacs, create the oraInst.loc file in any directory. The contents of the file consist of the following two lines:

```
inventory_loc=oui_inventory_directory
inst_group=oui_install_group
```

Replace *oui_inventory_directory* with the full path to the directory where you want the Installer to create the inventory directory. Replace *oui_install_group* with the name of the group whose members have write permissions to this directory.

3. Exit from the root user.

> **Note:** After you performing the silent installation on UNIX platforms, you must run the *ORACLE_HOME*/root.sh script as the root user. The root.sh script detects settings of environment variables and enables you to enter the full path of the local bin directory.

C.2.2 Windows Systems: Creating the Registry Key

If you have not installed Oracle Identity Management on your system, you must create the following Registry key and value:

```
HKEY_LOCAL_MACHINE / SOFTWARE / Oracle / inst_loc = [inventory_directory]
```

Replace *inventory_directory* with the full path to your Installer files. For example: C:\Program Files\Oracle\Inventory

C.3 Creating Response Files

Before performing a silent installation, you must provide information specific to your installation in a response file. Response files are text files that you can create or edit in a text editor. The Installer will fail if you attempt a silent installation using a response file that is not configured correctly.

Several default response files, which you can use as templates and customize for your environment, are included in the installation media. These default response files are located in the Disk1/stage/Response directory on UNIX, or in the Disk1\stage\Response directory on Windows.

Creating Response Files for Oracle Identity Management Software Installation

When you use the Oracle Identity Management Installation Wizard to install the software for the first time, you can save a summary of your installation in a response file.

To create a response file for Oracle Identity Management 11.1.1.3.0 software Installer for Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Authorization Policy Manager, and Oracle Identity Navigator, complete the following steps:

1. On the Installation Summary screen in the installation wizard, click **Save** in the **Save Response File** field.
2. When prompted, save the file to a local directory.

Creating Response Files for Oracle Identity Manager Configuration

When you use the Oracle Identity Manager Configuration Wizard to configure Oracle Identity Manager Server, Design Console, or Remote Manager for the first time, you can save a summary of your configuration in a response file.

To create this response file, complete the following steps:

1. On the Configuration Summary screen in the installation wizard, click **Save** in the **Save Response File** field.
2. When prompted, save the file to a local directory.

C.3.1 OID, OVD, ODSM, ODIP, and OIF

The following is a list of the default response files included in the installation media for the Oracle Identity Management Suite containing Oracle Internet Directory (OID), Oracle Virtual Directory (OVD), Oracle Directory Services Manager (ODSM), Oracle Directory Integration Platform (ODIP), and Oracle Identity Federation (OIF):

- im_install_only.rsp: Use this response file to install Oracle Identity Management components without configuring them.
- im_install_config.rsp: Use this response file to install and configure Oracle Identity Management components.
- im_config_only.rsp: Use this response file with the Oracle Identity Management 11g Release 1 (11.1.1) Configuration Wizard (config.sh script or config.bat) in *ORACLE_HOME*/bin/ to configure installed components.

C.3.2 OIM, OAM, OAAM, OAPM, and OIN

The following is a list of the default response files included in the installation media for the Oracle Identity Management Suite containing Oracle Identity Manager (OIM), Oracle Access Manager (OAM), Oracle Adaptive Access Manager (OAAM), Oracle Authorization Policy Manager (OAPM), and Oracle Identity Navigator (OIN):

- iamsuite_install_only.rsp: Use this response file to install Oracle Identity Management components without configuring them.
- iamsuite_config_only.rsp: Use this response file with the Oracle Identity Manager 11*g* Release 1 (11.1.1) Configuration Wizard (config.sh script or config.bat) in *ORACLE_HOME*/bin/ to configure Oracle Identity Manager Server, Design Console, and Remote Manager.
- deinstall_oh.rsp: Use this response file with the Oracle Identity Management 11*g* Release 1 (11.1.1) Deinstaller to deinstall installed components.

C.3.3 Securing Your Silent Installation

Your response files contain certain passwords required by the Installer. To minimize security issues regarding these passwords in the response file, follow these guidelines:

- Set the permissions on the response files so that they are readable only by the operating system user who will be performing the silent installation.
- If possible, remove the response files from the system after the silent installation is completed.

C.4 Performing a Silent Installation

To perform a silent Oracle Identity Management installation, you invoke the Installer with the -silent flag and provide a response file from the command line.

On UNIX

The following is the syntax for running the Installer from the command line on UNIX systems:

```
runInstaller [-mode] [-options] [(COMMAND_LINE_VARIABLE=VARIABLE_VALUE)*]
```

For example:

```
./runInstaller -silent -response FILE
```

On Windows

The following is the syntax for running the Installer from the command line on Windows systems:

```
setup.exe [-mode] [-options] [(COMMAND_LINE_VARIABLE=VARIABLE_VALUE)*]
```

For example:

```
setup.exe -silent -response FILE
```

C.5 Installer Command Line Parameters

Table C–1 lists and describes supported Installer command line parameters:

Table C–1 Installer Command Line Parameters

Parameter	Description
Installation Modes - Only One Mode Can be Specified	
-i | -install	Launches the Installer in GUI mode. This is the default mode and is used if no mode is specified on the command line.
-silent	Install in silent mode. The Installer must be passed either a response file or command line variable value pairs.
-d | -deinstall	Launches the Installer in GUI mode for deinstallation.
-p | -prerequisite	Launches the Installer in GUI mode but only checks the prerequisites. No software is installed.
-v | -validate	Launches the Installer in GUI mode and performs all prerequisite and validation checking, but does not install any software.
-sv | -silentvalidate	Performs all prerequisite and validation checking in silent mode. You must pass the Installer either a response file or a series of command line variable value pairs.
Installation Options	
-help | --help | --usage	Displays the usage parameters for the runInstaller command.
-invPtrLoc *file*	Pointer to the inventory location file. Replace file with the full path and name of the oraInst.loc file.
-response *file* | -responseFile *file*	Pointer to the response file. Replace file with the full path and name of the response file.
-jreLoc *location*	Pointer to the location where Java Runtime Environment (JRE) is installed. Replace *location* with the full path to the jre directory where your JRE is installed.

Table C–1 (Cont.) Installer Command Line Parameters

Parameter	Description
-logLevel *level*	Specify the level of logging performed by the Installer; all messages with a lower priority than the specified level will be recorded. Valid levels are: ■ severe ■ warning ■ info ■ config ■ fine ■ finer ■ finest
-debug	Obtain debug information from the Installer.
-force	Allow the silent installation to proceed in a non-empty directory.
-printdiskusage	Log debugging information pertaining to disk usage.
-printmemory	Log debugging information pertaining to memory usage.
-printtime	Log debugging information pertaining to time usage. This command causes the timeTakentimestamp.log file to be created.
-waitforcompletion	Windows only - the Installer will wait for completion instead of spawning the Java engine and exiting.
-noconsole	Messages will not be displayed to the console window.
-ignoreSysPrereqs	Ignore the results of the system prerequisite checks and continue with the installation.
-executeSysPrereqs	Execute the system prerequisite checks only, then exit.
-paramFile *file*	Specify the full path to the oraparam.ini file. This file is the initialization file for the Installer. The default location of this file is Disk1/install/platform.
-novalidation	Disables all validation checking performed by the Installer.
-nodefaultinput	For the GUI install, several screens have information or default values pre-populated. Specifying this option disables this behavior so that no information or values are pre-populated.
Command Line Variables	
Installer Variables	Installer variables are specified using *varName=value*. For example: `ORACLE_HOME=/scratch/install/Oracle_IDM1`
Session Variables	Session variables are specified using session:*varName=value*

D

Troubleshooting the Installation

This appendix describes solutions to common problems that you might encounter when installing Oracle Identity Management. It contains the following topics:

- General Troubleshooting Tips
- Installation Log Files
- Configuring OIM Against an Existing OIM 11g Schema
- Need More Help?

D.1 General Troubleshooting Tips

If you encounter an error during installation:

- Consult the Oracle Fusion Middleware 11*g* Release 1 (11.1.1). You can access the Release Notes on the Oracle Technology Network (OTN) Documentation Web site. To access this Web site, go to the following URL:

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

- Verify your system and configuration is certified. See System Requirements and Certification for more information.
- Verify your system meets the minimum system requirements. See System Requirements and Certification for more information.
- Verify you have satisfied the dependencies for the deployment you are attempting. Each deployment documented in this guide contains a "Dependencies" section.
- If you entered incorrect information on one of the installation screens, return to that screen by clicking **Back** until you see the screen.
- If an error occurred while the Installer is copying or linking files:
  1. Note the error and review the installation log files.
  2. Remove the failed installation. See "Deinstalling Oracle Identity Management" on page A-1 for more information.
  3. Correct the issue that caused the error.
  4. Restart the installation.
- If an error occurred while configuring Oracle Identity Manager using the Oracle Identity Manager Configuration Wizard:
  1. Note the error and review the configuration log files.

2. Verify whether the dependencies are met. For example, Administration Server and Database should be up and running.
3. Correct the issue that caused the error.
4. Restart the Oracle Identity Manager Configuration Wizard.

D.2 Installation Log Files

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

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

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

The server log files are created in the <DOMAIN_HOME>/server/<servername/logs directory.

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

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

D.3 Configuring OIM Against an Existing OIM 11*g* Schema

In this scenario, you have created and loaded the appropriate Oracle Identity Manager (OIM) schema, installed and configured Oracle Identity Manager in a new or existing WebLogic domain. During domain configuration, you have configured JDBC Component Schemas by using the Oracle Fusion Middleware Configuration Wizard.

If you want to configure Oracle Identity Manager in a second WebLogic domain against the existing Oracle Identity Manager 11*g* schemas, you must complete the following steps when you try to configure Oracle Identity Manager using the Oracle Identity Manager Configuration Wizard:

1. When prompted, you must copy the `.xldatabasekey` file from the first WebLogic domain directory (`/<MW_HOME>/user_projects/domains/<name_of_your_first_oim_domain>/config/fmwconfig/`) to the second WebLogic domain directory (`/<MW_HOME>/user_projects/domains/<name_of_your_second_oim_domain>/config/fmwconfig/`). Proceed with the Oracle Identity Manager configuration.
2. After configuring Oracle Identity Manager using the Oracle Identity Manager Configuration Wizard, copy the `cwallet.so`, `default_keystore.jks`, and `xlserver.crt` files from the first WebLogic domain directory (`/<MW_HOME>/user_projects/domains/<name_of_your_first_oim_domain>/config/fmwconfig/`) to the second domain Home directory (`/<MW_HOME>/user_projects/domains/<name_of_your_second_oim_domain>/config/fmwconfig/`).

3. After copying the files, start the Oracle Identity Manager Managed Server, as described in Starting the Stack.

D.4 Need More Help?

If you cannot solve a problem using the information in this appendix, look for additional information in My Oracle Support (formerly MetaLink) at `http://metalink.oracle.com`.

If you cannot find a solution to your problem, open a service request.

E

OAAM Partition Schema Reference

This appendix provides information about tables and stored procedures used with Oracle Adaptive Access Manager (OAAM) with Partition support.

It contains the following topics:

E.1 Overview

Database tables in the Oracle Adaptive Access Manager database are divided into the following categories:

- Static partition tables
- Transactional partition tables
- Non-partitioned tables

Note: All the tables contain the composite partition (RANGE, HASH). The Range partition is created using CREATE_TIME while the HASH key is defined based on application logic.

lists the Oracle Adaptive Access Manager (OAAM) partition tables. All the other tables are non-partitioned.

Table E–1 OAAM Database Partition Tables

Table Type	Frequency	Table Name
Static Partition	Monthly	V_USER_QA
		V_USER_QA_HIST
Transactional Partition	Monthly	VCRYPT_TRACKER_NODE_HISTORY
		VCRYPT_TRACKER_USERNODE_LOGS
		VCRYPT_TRACKER_NODE
		VT_USER_DEVICE_MAP
		V_MONITOR_DATA
		VT_SESSION_ACTION_MAP
		VT_ENTITY_ONE
		VT_ENTITY_ONE_PROFILE
		VT_USER_ENTITY1_MAP
		VT_ENT_TRX_MAP
		VT_TRX_DATA
		VT_TRX_LOGS
Transactional Partition	Weekly	VR_POLICYSET_LOGS
		VR_POLICY_LOGS
		VR_RULE_LOGS
		VR_MODULE_LOGS

E.2 Partition Add Maintenance

After the initial Oracle Adaptive Access Manager repository setup, the following stored procedures are set up as dbms_jobs to maintain the partitions on a regular basis:

- Sp_Oaam_Add_Monthly_Partition
- Sp_Oaam_Add_Weekly_Partition

E.2.1 Sp_Oaam_Add_Monthly_Partition

This stored procedure adds partitions for tables with the monthly frequency.

The script runs at the end of each month to create partitions for the following month. To simultaneously add partitions for subsequent months, the partitions are added based on the partition of the previous month.

If this stored procedure fails to exceute (if your monthly partition is missing), you may see database errors, `"ORA-14400 and ORA-14401,"` forcing the Oracle Adaptive Access Manager application to stop.

E.2.2 Sp_Oaam_Add_Weekly_Partition

This stored procedure adds partitions for tables with the weekly frequency.

The script runs at the end of each week to create partitions for the following week. To simultaneously add partitions for subsequent weeks, the partitions are added based on the partition of the previous week.

If this stored procedure fails to exceute (if your weekly partition is missing), you may see database errors, "ORA-14400 and ORA-14401," forcing the Oracle Adaptive Access Manager application to stop.

E.3 Partition Maintenance Scripts

After the initial Oracle Adaptive Access Manager repository setup, use the following scripts with purging or archiving maintenance scripts to maintain the partitions on a regular basis:

- drop_monthly_partition_tables.sql
- drop_weekly_partition_tables.sql
- add_monthly_partition_tables.sql
- add_weekly_partition_tables.sql

The above mentioned scripts are located at <IDM_ORACLE_HOME>\oaam\oaam_db_maint_scripts\oaam_db_partition_maint_scripts

Note: You do not have to execute partition add scripts. You should only use them to create partitions manually because other automated dbms_jobs create partitions at regular intervals.

E.3.1 drop_monthly_partition_tables.sql

You can use this script to drop partitions for tables with the monthly frequency. You should run this script at the end of each month to drop partitions older than sixth months, based on the requirements of the Oracle Adaptive Access Manager application. Note that these tables will have six partitions at a given time.

E.3.2 drop_weekly_partition_tables.sql

You can use this script to drop partitions for tables with the weekly frequency. You should run this script either at the end of every fourteenth day or at the end of third week from the day the Oracle database was created to the dropping of partitions older than two weeks, based on the requirements of the Oracle Adaptive Access Manager application.

E.3.3 add_monthly_partition_tables.sql

You can use this script to add partitions for tables with the monthly frequency. You should run this script at the end of each month to create partitions for the following month. To add partitions for subsequent months at the same time, run this script multiple times. When you run the script multiple times, partitions are added based on the previous month's partition.

E.3.4 add_weekly_partition_tables.sql

You can use this script to add partitions for tables with the weekly frequency. You should run this script at the end of each month to create partitions for the following week. To add partitions for subsequent weeks at the same time, run this script multiple times. When you run the script multiple times, partitions are added based on the previous week's partition.

F

Oracle Identity Management 11.1.1.3.0 Software Installation Screens

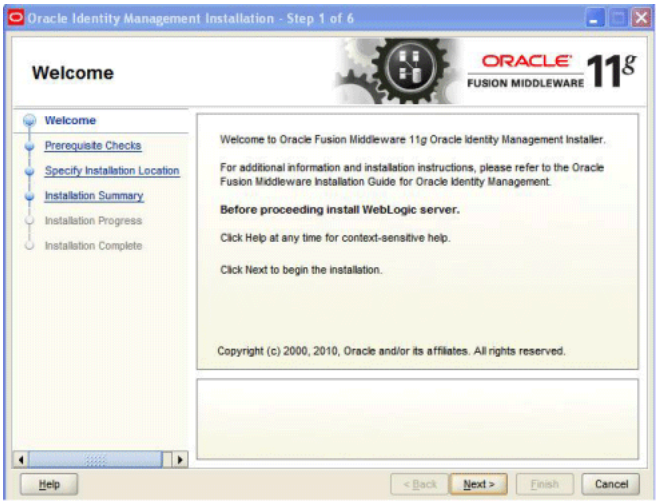
This appendix describes the screens of the Oracle Identity Management 11*g* software Installation Wizard that enables you to install Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Authorization Policy Manager, and Oracle Identity Navigator.

It contains the following topics:

F.1 Welcome

The Welcome screen is displayed each time you start the Oracle Identity Management 11*g* Installer wizard.

Figure F–1 Welcome Screen



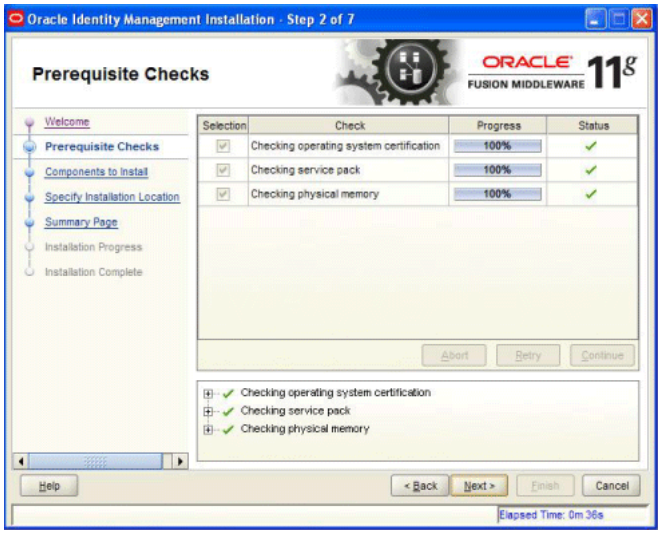
Click **Next** to continue.

F.2 Prerequisite Checks

The installation program ensures that you have a certified version, the correct software packages, sufficient space and memory to perform the operations that you have selected. If any issues are detected, errors appear on this page.

The following example screen applies to Windows operating systems only. For more information about prerequisite checks performed by the Installer, see Prerequisite Checks Performed by the Oracle Identity Management Installer.

Figure F–2 Prerequisite Checks Screen



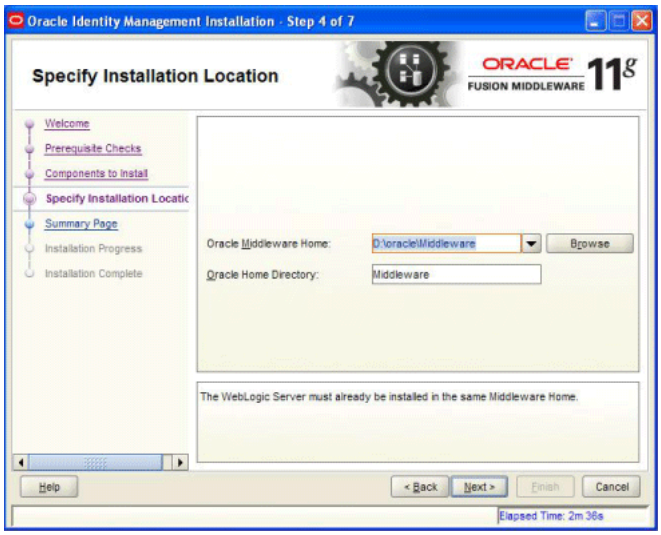
On this screen, you can select to **Abort**, **Retry**, or **Continue** with the installation.

If all the prerequisite checks pass inspection, click **Next** to continue.

F.3 Specify Installation Location

In this screen, you enter a location for the new Oracle Identity Management 11*g* software being installed.

Figure F–3 Specify Installation Location Screen



Ensure that Oracle WebLogic Server is already installed on your machine. Navigate to the Oracle Fusion Middleware Home directory by clicking **Browse**. Enter a name for the new Oracle Home directory for Oracle Identity Management 11g components.

If the Middleware location does not exist, you must install WebLogic Server and create a Middleware Home directory, as described in Installing Oracle WebLogic Server 10.3.3 and Creating the Oracle Middleware Home, before running the Oracle Identity Management Installer.

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

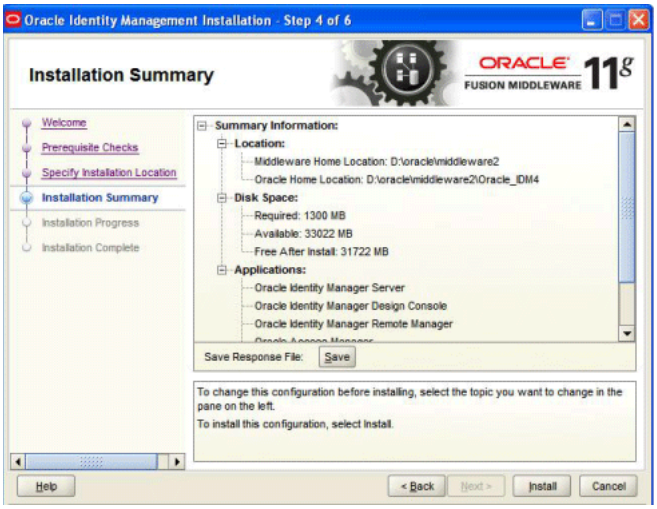
If you want to install only Oracle Identity Manager Design Console or Remote Manager, you do not need to install Oracle WebLogic Server or create a Middleware Home directory on the machine where Design Console or Remote Manager is being configured.

Click **Next** to continue.

F.4 Installation Summary

This screen displays a summary of your Oracle Identity Management 11*g* installation.

Figure F–4 Installation Summary Screen

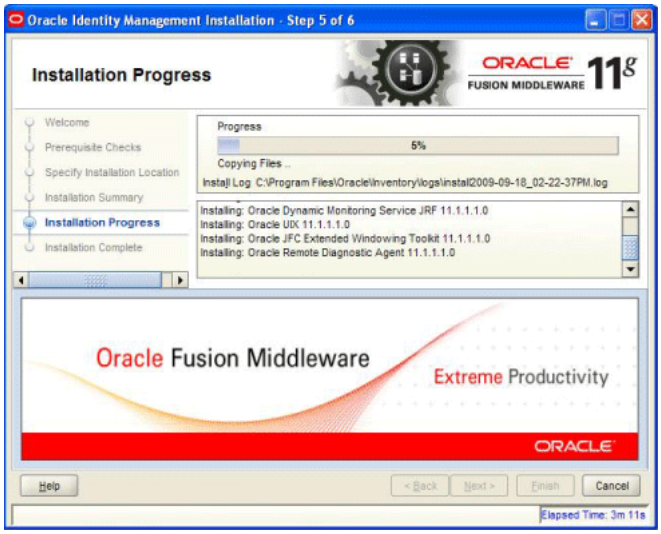


Review the contents of this screen, and click **Install** to start installing the Oracle Identity Management 11g software.

F.5 Installation Progress

This screen displays the progress of the Oracle Identity Management installation.

Figure F–5 Installation Progress Screen

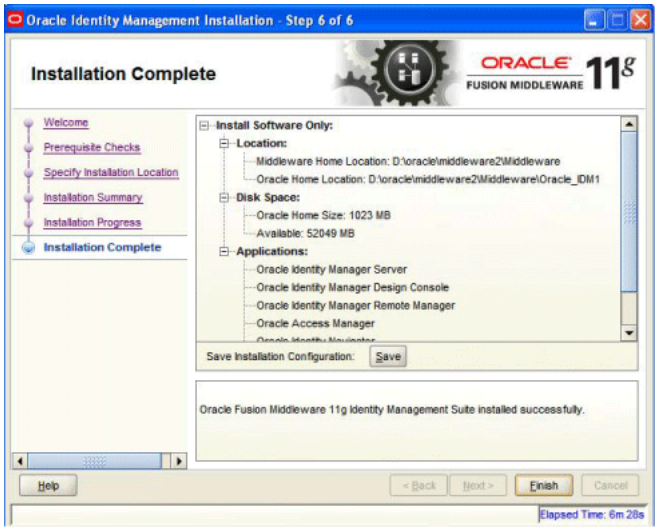


If you want to quit before the installation is completed, click **Cancel**. The installation progress indicator gives a running inventory of the files that are being installed. If you are only installing the software binaries, installation is complete after all of the binaries have been installed.

F.6 Installation Complete

This screen displays a summary of the installation parameters, such as Location, Disk Space, and Applications. To save the installation configuration in a response file, which is used to perform silent installations, click **Save**.

Figure F–6 Installation Complete Screen



Click **Finish** to complete the installation process.

G

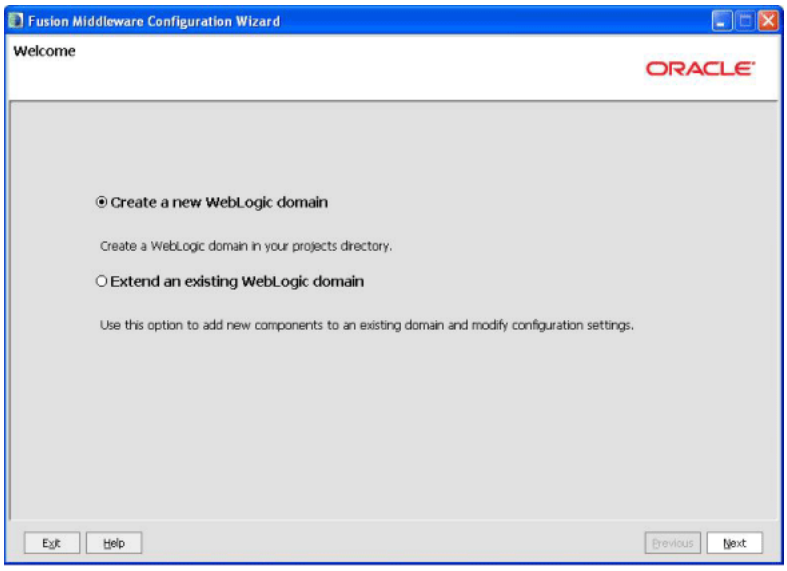
WebLogic Domain Configuration Screens

This appendix describes the screens of the Oracle Fusion Middleware Configuration Wizard that enables you to create or extend a WebLogic administration domain. This appendix contains the following topics:

G.1 Welcome

The Welcome screen is displayed each time you start the Oracle Fusion Middleware Configuration Wizard.

Figure G–1 Welcome Screen



Select **Create a new WebLogic domain** to create a new WebLogic domain in your projects directory.

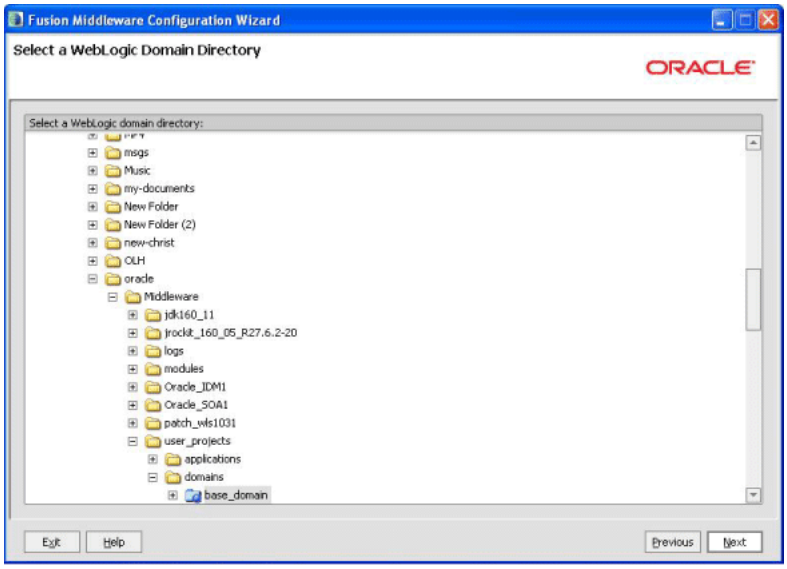
Select **Extend an existing WebLogic domain** if you want to add applications and services, or to override existing database access (JDBC) and messaging (JMS) settings.

Click **Next** to continue.

G.2 Select a WebLogic Domain Directory

This screen is displayed only if you choose to extend an existing WebLogic domain to support the new products.

Figure G–2 Select a WebLogic Domain DIrectory Screen



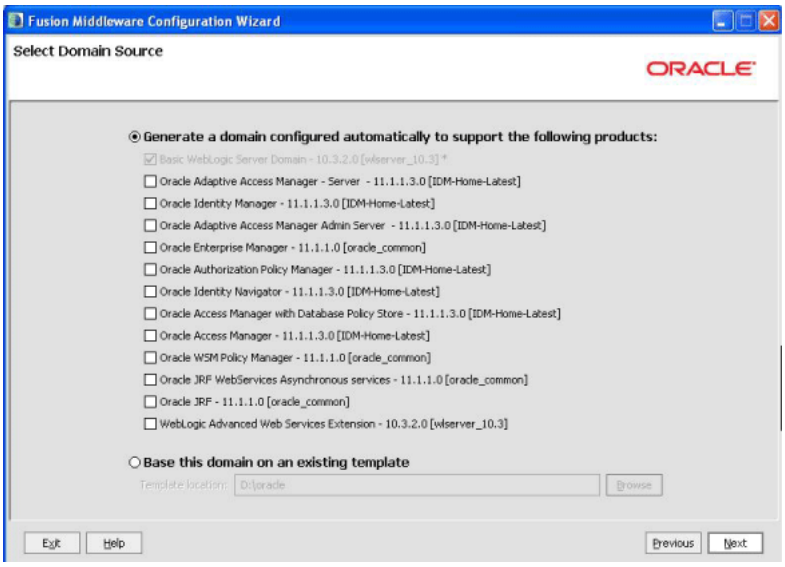
Select the WebLogic Domain directory to which you want to add your applications, or services, or both.

Click **Next** to continue.

G.3 Select Domain Source

The Select Domain Source screen enables you to select a domain source from which you want to create a new domain.

Figure G–3 Select Domain Source Screen



Select **Generate a domain configured automatically to support the following products:** to create your domain to support selected products. Then, select the products for which you want support.

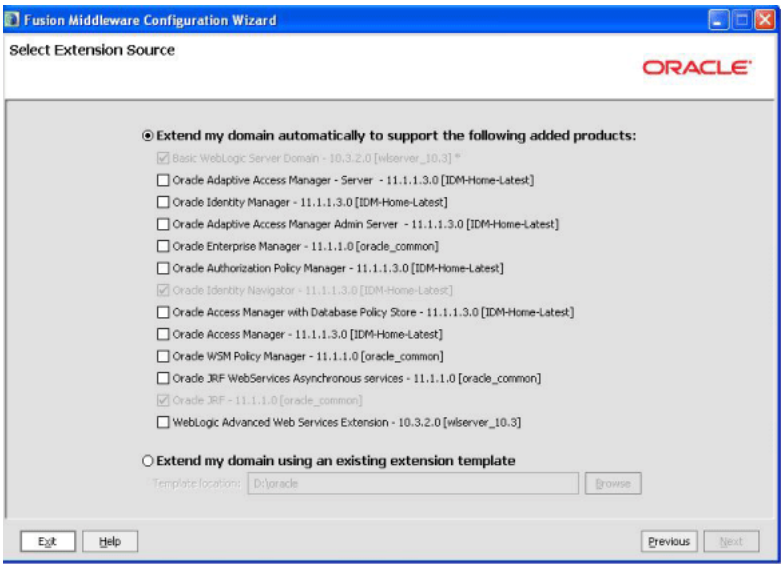
Select **Base this domain on an existing template** to create your domain based on an existing domain template. By default, domain templates for Oracle Identity Management 11*g* components are located in your `ORACLE_HOME\common\templates\applications` directory. Click **Browse** to navigate your directories to find an existing template.

Click **Next** to continue.

G.4 Select Extension Source

This screen is displayed only if you choose to extend an existing WebLogic domain to support the new products.

Figure G–4 Select Extension Source Screen



Select **Extend my domain automatically to support the following added products:** to extend your domain to support selected products. Then, select the products for which you want support.

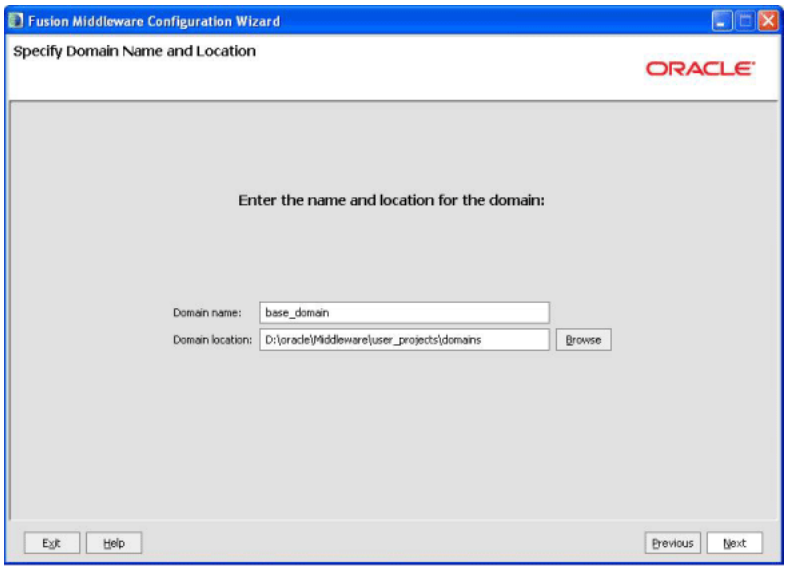
Select **Extend my domain using an existing extension template** to extend your domain based on an existing extension template. Click **Browse** to navigate your directories to find an existing template.

Click **Next** to continue.

G.5 Specify Domain Name and Location

In this screen, you enter a name and location for the new WebLogic domain being created.

Figure G–5 Specify Domain Name and Location Screen



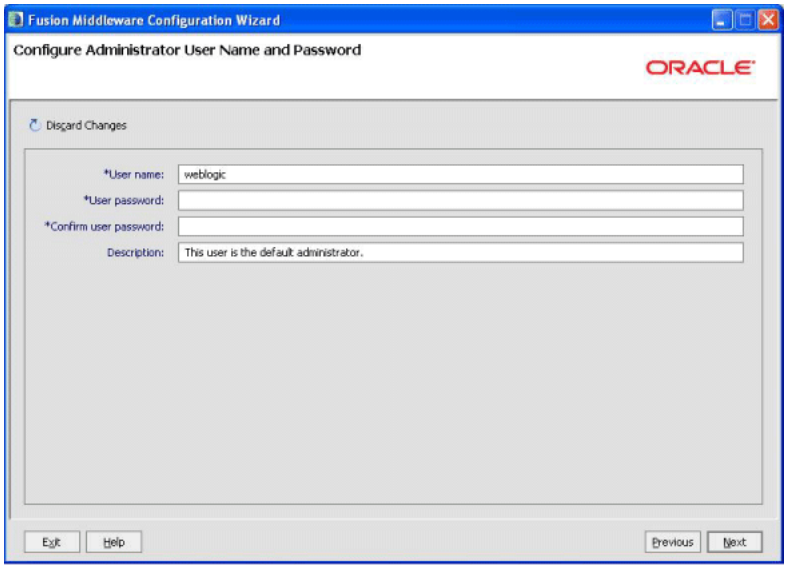
Enter a name for the new WebLogic domain, and select the location where the new domain must be created.

Click **Next** to continue.

G.6 Configure Administrator User Name and Password

This screen is displayed only if you choose to create a new WebLogic domain.

Figure G–6 Configure Administrator User Name and Password Screen



Create a user that will be assigned to the Administrator role. This user is the default administrator used to start development mode servers.

- **User name** - Specify the user name.

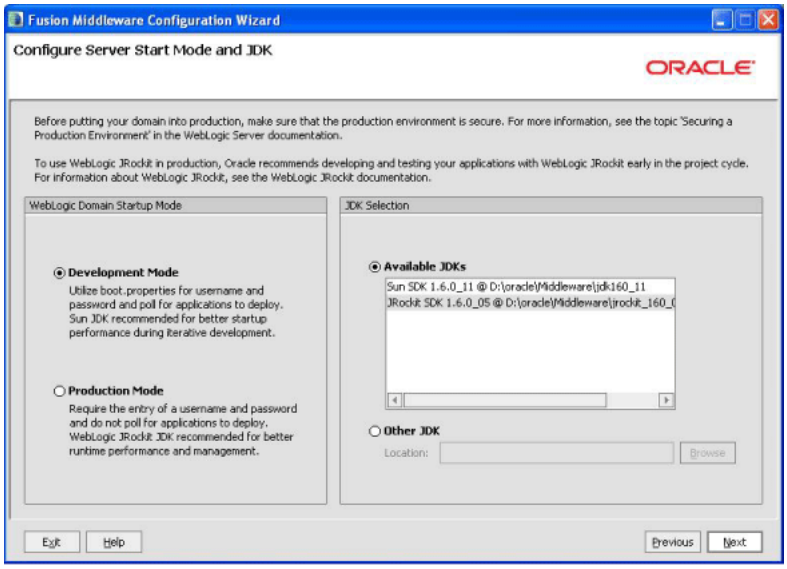
- **User password** - Specify the password for the user.
- **Confirm user password** - Re-enter the user password.
- **Description** - Enter a description for the user. This field is optional.

Click **Next** to continue.

G.7 Configure Server Start Mode and JDK

This screen is displayed only if you choose to create a new WebLogic domain.

Figure G–7 Configure Server Start Mode and JDK Screen



In the WebLogic Domain Startup Mode section, select one of the following startup modes:

- Development Mode

  In this mode, `boot.properties` is used for user names and passwords, and polling is used for application deployment. Sun JDK is the default for this mode.

- Production Mode

  In this mode, user names and passwords are required, and polling is not used for application deployment. WebLogic JRockit JDK is the default for this mode.

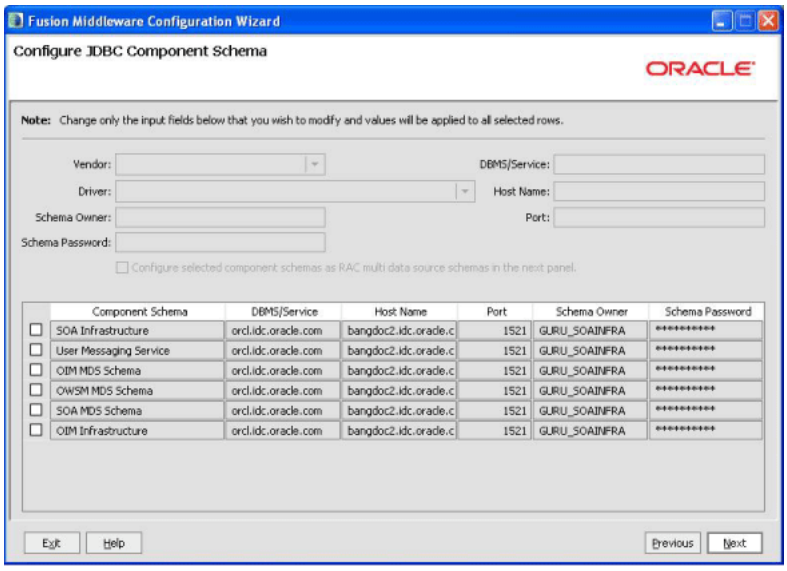
In the JDK Selection section, select a JDK from the list of available JDKs, or select **Other JDK** and click **Browse** to find another JDK on your system.

Click **Next** to continue.

G.8 Configure JDBC Component Schema

This screen is displayed only if you choose to extend an existing WebLogic domain to support a new product.

Figure G–8 Configure JDBC Component Schema Screen



Use this screen to edit the configuration information for each JDBC data source.

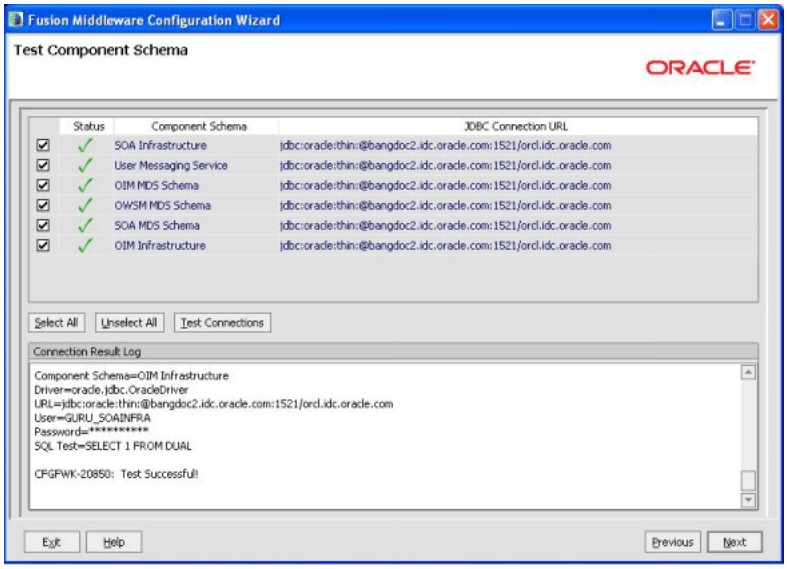
A data source contains a pool of database connections. Your application uses a data source by looking it up in the JNDI tree, requesting a connection, using the connection, and then returning the connection to the data source.

Click **Next** to continue.

G.9 Test Component Schema

This screen displays the test results.

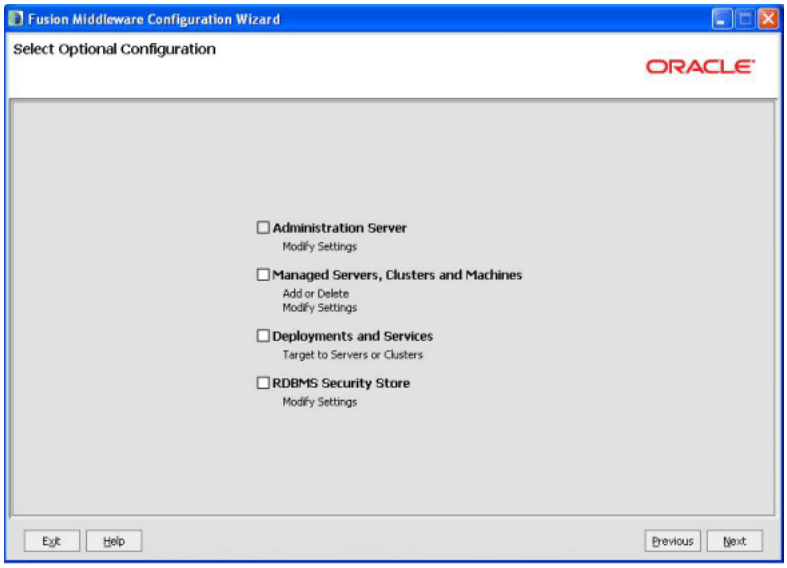
Figure G–9 Test Component Schema Screen



G.10 Select Optional Configuration

This screen provides you with options to configure and customize any of the server or cluster settings listed.

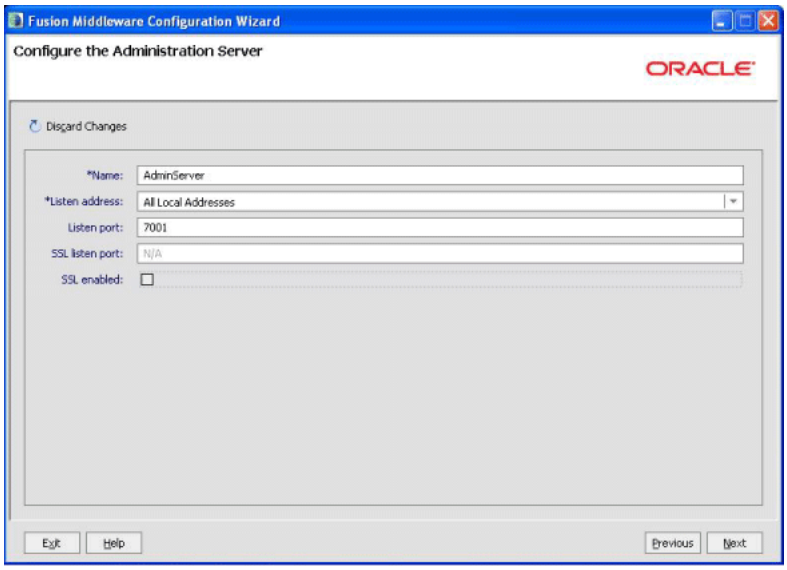
Figure G–10 Select Optional Configuration Screen



G.11 Configure the Administration Server

This screen is displayed only if you choose to create a new WebLogic domain.

Figure G–11 Configure the Administration Server Screen



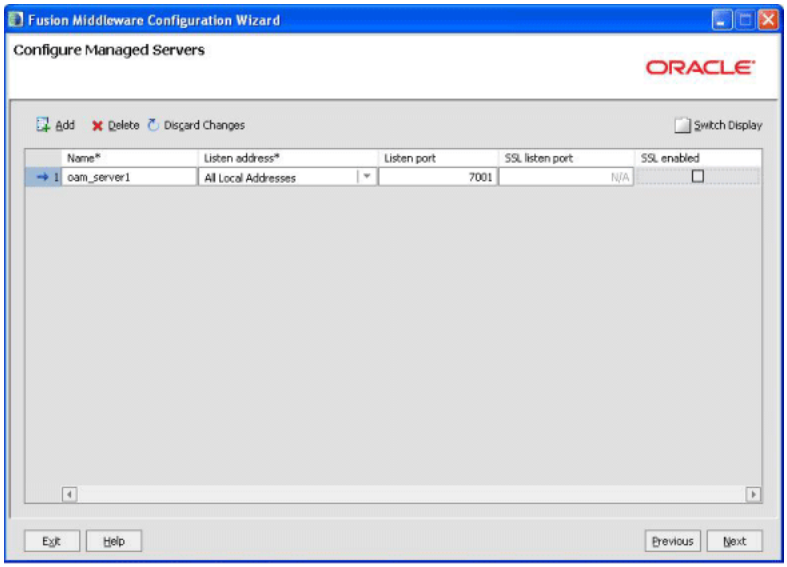
Each WebLogic Server domain must have one Administration Server, which hosts the Administrative Console used to perform administration tasks.

Click **Next** to continue.

G.12 Configure Managed Servers

This screen enables you to configure Managed Servers. A Managed Server is an instance of Oracle WebLogic Server used to host enterprise applications. A typical production environment has at least one Managed Server.

Figure G–12 Configure Managed Servers Screen



Use this screen to add or delete Managed Servers. For each Managed Server, specify:

- Name

  Name of the Managed Server.

- Listen Address

  Select an address from the drop-down list; the server will listen on the specified addresses.

- Listen Port

  Listen port number.

- SSL Listen Port

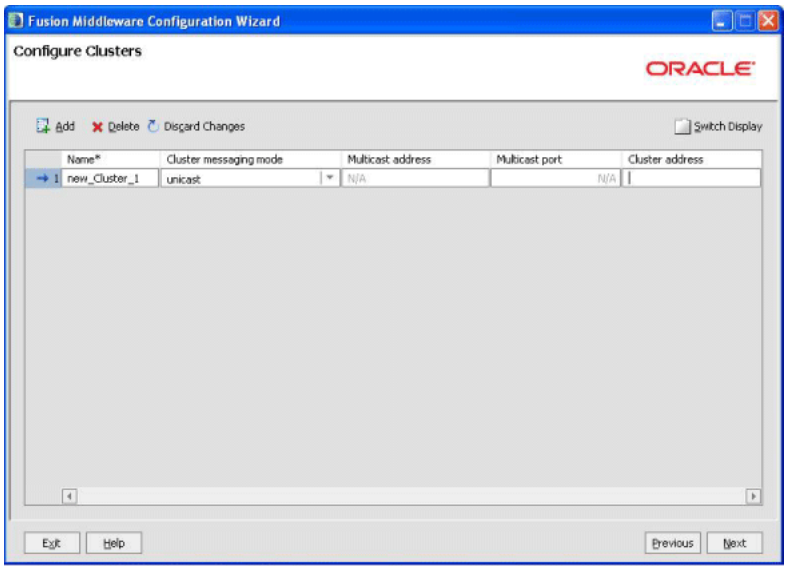
  Port number for SSL connections - this column is only active if the corresponding "SSL enabled" check box in the same row is selected.

Click **Next** to continue.

G.13 Configure Clusters

This screen enables you to configure clusters. A cluster contains multiple WebLogic Server instances running simultaneously and working together for scalability and reliability. To clients, a cluster appears as a single WebLogic Server instance.

Figure G–13 Configure Clusters Screen



Use this screen to add or delete configuration information for clusters.

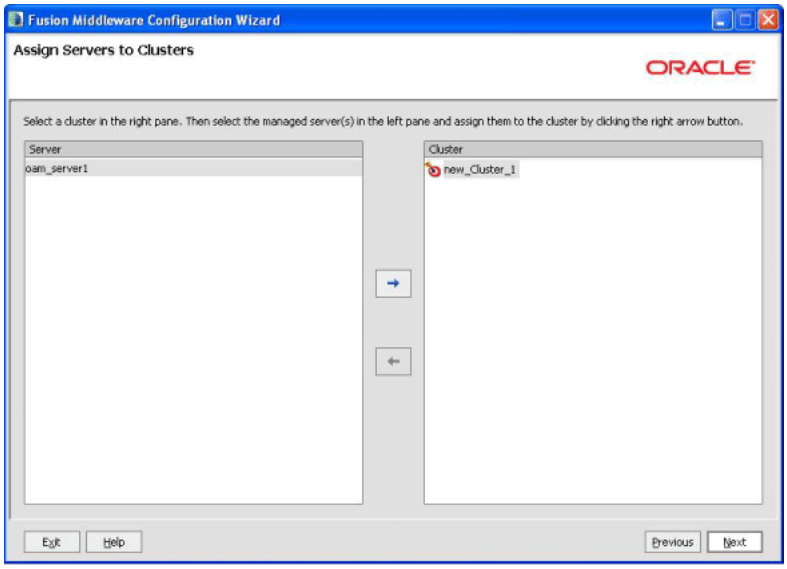
For more information about configuring clusters for Oracle Identity Management products, see the "Configuring High Availability for Identity Management Components" topic in the guide *Oracle Fusion Middleware High Availability Guide*.

Click **Next** to continue.

G.14 Assign Servers to Clusters

This screen enables you to assign a Managed Server to the cluster. This screen is required only if you choose to use Node Manager.

Figure G–14 Assign Servers to Clusters Screen



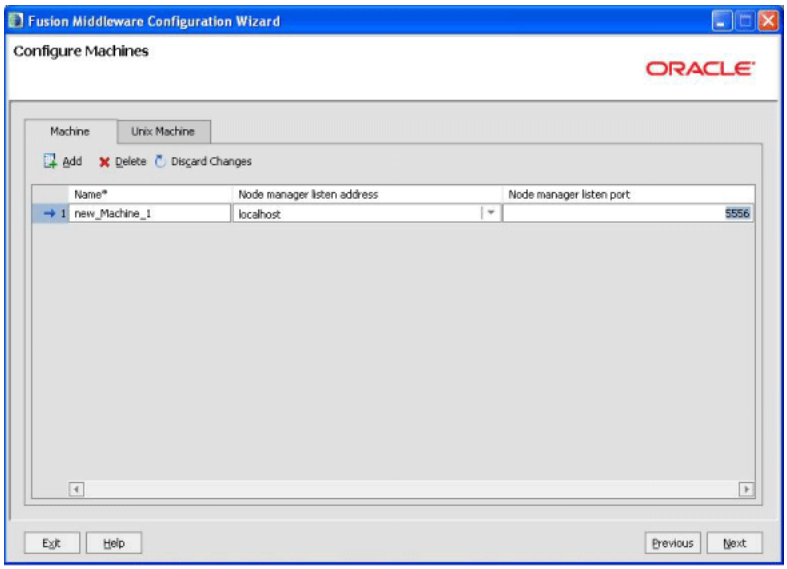
Select a cluster in the right pane, and select a Managed Server in the left pane. Assign the Managed Server to the cluster by clicking the right arrow button.

Click **Next** to continue.

G.15 Configure Machines

This screen enables you to configure machines that host WebLogic Servers.

Figure G–15 Configure Machines Screen



Use this screen to add or delete machines.

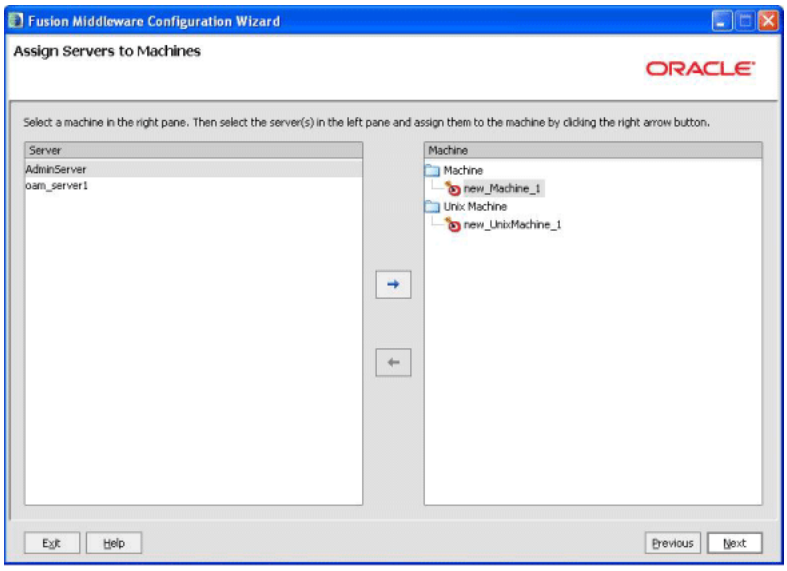
The Administration Server and Node Manager use the machine definition on this screen to start remote servers.

Click **Next** to continue.

G.16 Assign Servers to Machines

This screen enables you to assign each WebLogic Server instance to the corresponding machine on which it runs.

Figure G–16 Assign Servers to Machines Screen



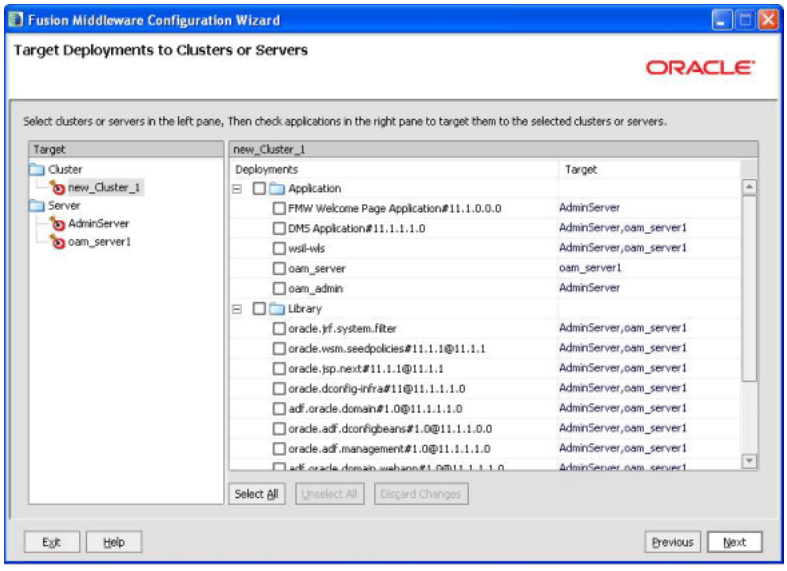
Select a machine in the right pane, and select a server in the left pane. Assign the server to the machine by clicking the right arrow button.

Click **Next** to continue.

G.17 Target Deployments to Clusters or Servers

This screen enables you to target your deployments to servers or clusters. Doing so enables WebLogic Server to serve the deployment to clients.

Figure G–17 Target Deployments to Clusters or Servers



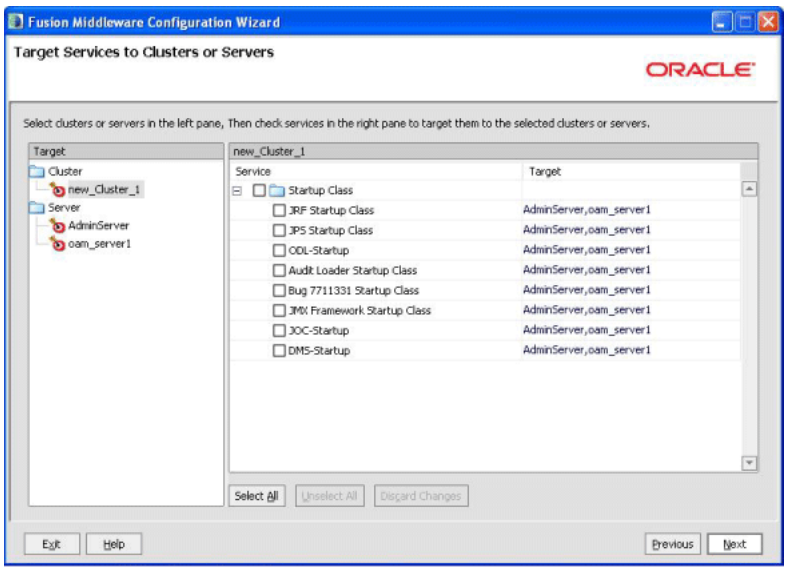
Select clusters or servers in the left pane, and select the check boxes corresponding to applications in the right pane to target them to the selected clusters or servers.

Click **Next** to continue.

G.18 Target Services to Clusters or Servers

This screen enables you to target your services (for example, JMS, JDBC, startup and shutdown classes) to servers or clusters. Doing so enables your applications to use these services. It is an optional task.

Figure G–18 Target Services to Clusters or Servers Screen



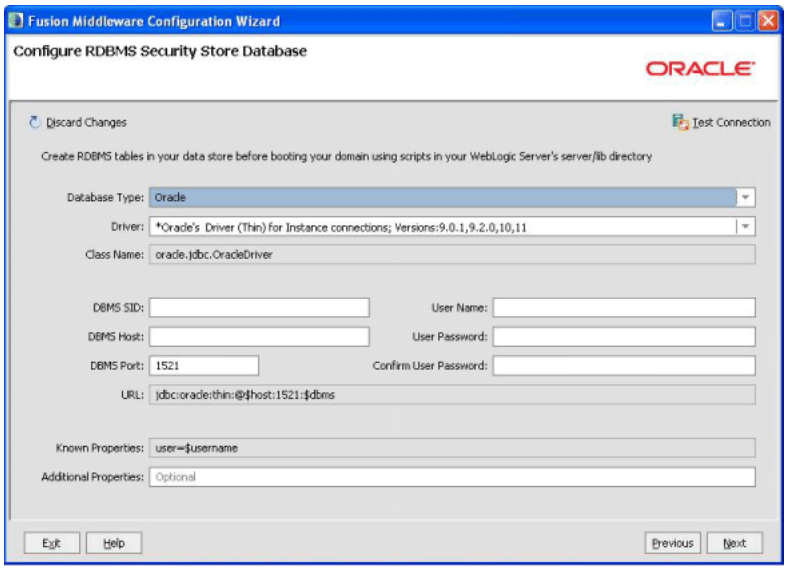
Select clusters or servers in the left pane, and select the check boxes corresponding to services in the right pane to target them to the selected clusters or servers.

Click **Next** to continue.

G.19 Configure RDBMS Security Store Database

This screen enables you to configure an RDBMS security store database.

Figure G–19 Configure RDBMS Security Store Database



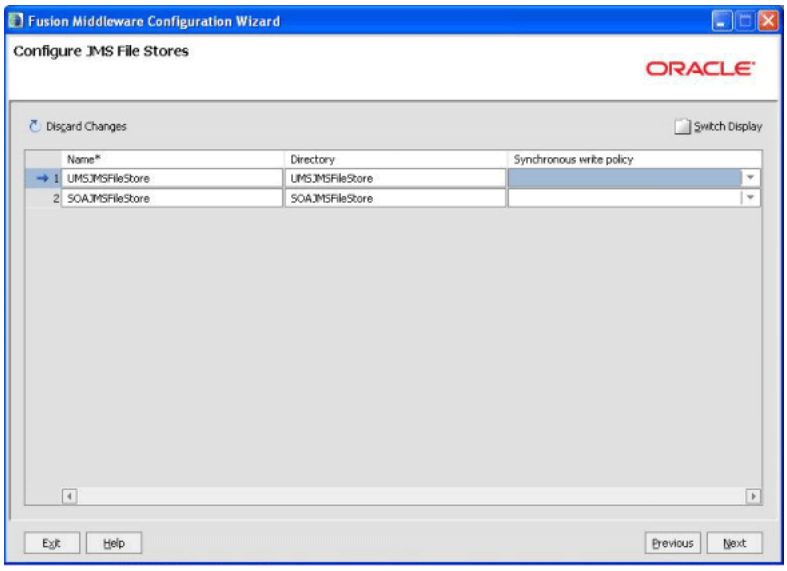
Make changes to your RDBMS. Make sure that your RDBMS tables are created prior to booting your domain. The scripts used by the DBA are located in the WebLogic Server server/lib directory.

After entering information in the fields, click **Next** to continue.

G.20 Configure JMS File Stores

This screen is displayed only if you choose to extend an existing WebLogic domain to support the new product.

Figure G–20 Configure JMS File Stores Screen



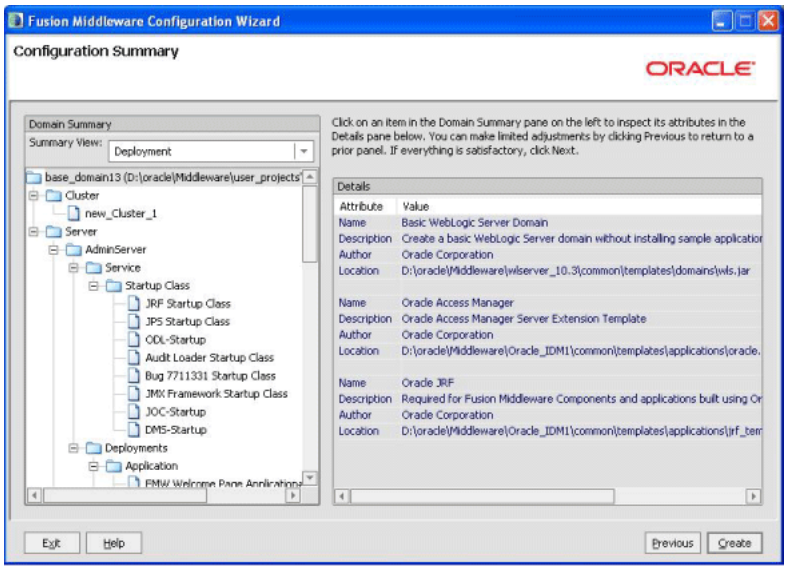
In this screen, you can configure a JMS file store. In addition, you can select a synchronous write policy: Cache-Flush, Direct-Write, or Disabled

Click **Next** to continue.

G.21 Configuration Summary

This screen displays a summary of your domain configuration.

Figure G–21 Configuration Summary Screen



Review the contents of your domain.

Click **Create** to start configuring your domain.

H

Oracle Identity Manager Configuration Screens

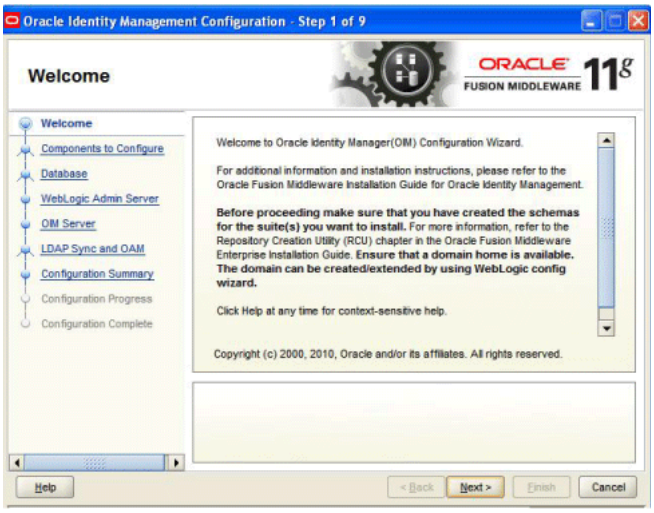
This appendix describes the screens of the Oracle Identity Manager 11*g* Configuration Wizard that enables you to configure Oracle Identity Manager Server, Oracle Identity Manager Design Console, and Oracle Identity Manager Remote Manager.

This appendix contains the following topics:

H.1 Welcome

The Welcome screen is displayed each time you start the Oracle Identity Manager Configuration Wizard.

Figure H–1 Welcome Screen



You can use the Oracle Identity Manager Configuration Wizard only once during initial setup for configuring Oracle Identity Manager Server. After configuring Oracle Identity Manager Server using this wizard, you cannot re-run this wizard to modify the configuration of Oracle Identity Manager. You must use Oracle Enterprise Manager Fusion Middleware Control to make such modifications. However, you can run this wizard on other machines, where Design Console or Remote Manager is configured, as and when needed.

Ensure that you have configured Oracle Identity Manager in a new or existing WebLogic domain before launching the Oracle Identity Manager Configuration Wizard to configure Oracle Identity Manager Server, Design Console on Windows, and Remote Manager.

If you are configuring Server, you must run this wizard on the machine where the WebLogic Administration Server is running (the Administration Server for the domain in which Oracle Identity Manager is deployed). Ensure that the Administration Server is up and running before you start configuring Oracle Identity Manager Server.

If you are configuring only Design Console, you must run this wizard on the Windows machine where Design Console should be configured. If you are configuring only Remote Manager, you must run this wizard on the machine where Remote Manager is being configured. Note that the Oracle Identity Manager Server should be configured before you can configure Design Console or Remote Manager.

Click **Next** to continue.

H.2 Components to Configure

Use this screen to select the Oracle Identity Manager components that you want to configure. Oracle Identity Manager components include Server, Design Console, and Remote Manager.

Before configuring Oracle Identity Manager Server, Design Console or Remote Manager, ensure that you have configured Oracle Identity Manager in a new or existing WebLogic domain using the Oracle Fusion Middleware Configuration Wizard.

Figure H–2 Components to Configure Screen

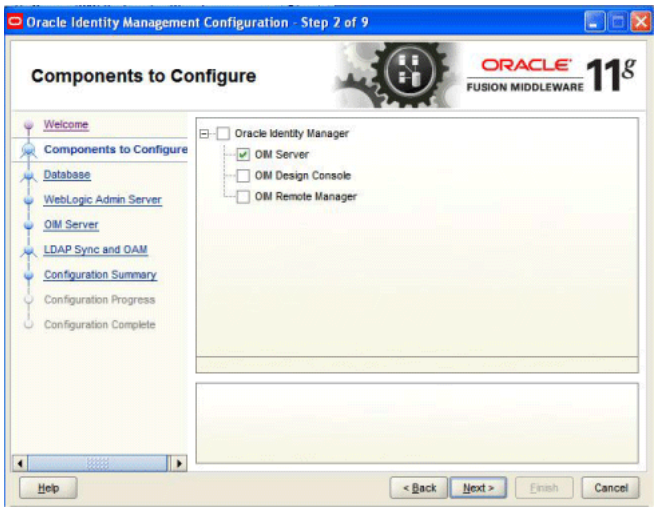


Table H–1 describes the Oracle Identity Manager components that you can choose.

Table H–1 Oracle Identity Manager Configuration Choices

Option	Description
Configure all components on this screen	To configure Oracle Identity Manager Server, Design Console, and Remote Manager simultaneously on the same machine, select the **Oracle Identity Manager** option.
Configure only Oracle Identity Manager Server	To configure only Oracle Identity Manager Server, select the **OIM Server** option. This option is selected, by default. Note that WebLogic Administration Server for the domain (the domain in which Oracle Identity Manager is deployed) should be up and running.
Configure only Oracle Identity Manager Design Console	To configure only Oracle Identity Manager Design Console, select the **OIM Design Console** option. However, note that Oracle Identity Manager Server must be configured either on the local machine or on a remote machine before you can run Design Console on development machines. Design Console is supported on Windows operating systems only.
Configure only Oracle Identity Manager Remote Manager	To configure only Oracle Identity Manager Remote Manager, select the **OIM Remote Manager** option. However, note that Oracle Identity Manager Server must be configured either on the local machine or on a remote machine before you can run Remote Manager.

Note: You can also select any combination of two of the three Oracle Identity Manager components.

H.3 Database

In this screen, you specify the database and schema information. Note that you should have created and loaded Oracle Identity Manager schemas using the Oracle Fusion Middleware Repository Creation Utility (RCU) before configuring Oracle Identity Manager Server. For information about creating and loading Oracle Identity Manager schemas, see Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU).

Figure H–3 Database Screen

You can use the same database or different databases for creating the Oracle Identity Manager schema and the Metadata Services schema.

Table H–2 describes the database connection information that you must specify.

Table H–2 Fields in the Database Screen

Field	Description

Connect String	Enter the full path, listen port, and service name for your Oracle database. For a single host instance, the format of connect string is `hostname:port:servicename`.
	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:instancename1^host2:port2:instancename2@servicename`

OIM Schema User Name	Enter the name of the schema user that you created for Oracle Identity Manager using the Oracle Fusion Middleware Repository Creation Utility. If you upgraded your existing Oracle Identity Manager schema to 11*g* Release 1 (11.1.1), enter the user name for your existing schema.
OIM Schema Password	Enter the password for the Oracle Identity Manager schema user that you set while creating the schema using the Oracle Fusion Middleware Repository Creation Utility (RCU). If you upgraded your existing Oracle Identity Manager schema to 11*g* Release 1 (11.1.1), enter the password for your existing schema.
Select different database for MDS schema	Select this check box if you want to use a different database for the Metadata Services (MDS) schema.

Table H–2 (Cont.) Fields in the Database Screen

Field	Description
MDS Connect String	If you are using a different database for the Metadata Services (MDS) schema, enter the full path, listen port, and service name for the database associated with the MDS schema. The format of the connect string is similar to that of the standard Connect String.
MDS Schema User Name	Enter the name of the schema user that you created for **AS Common Services - Metadata Services** by using the Oracle Fusion Middleware Repository Creation Utility (RCU). If you upgraded your existing Metadata Services schema to 11*g* Release 1 (11.1.1), enter the user name for your existing schema.
MDS Schema Password	Enter the password for the **AS Common Services - Metadata Services** schema user that you set while creating the schema by using the Oracle Fusion Middleware Repository Creation Utility (RCU). If you upgraded your existing Oracle Identity Manager schema to 11*g* Release 1 (11.1.1), enter the password for your existing schema.

After entering information in the fields, click **Next** to continue.

H.4 WebLogic Admin Server

In this screen, you specify the t3 URL, user name and password for the WebLogic administration domain in which the Oracle Identity Manager application is deployed. Ensure that the Administration Server is up and running.

Figure H–4 WebLogic Admin Server Screen

In the **WebLogic Admin Server URL** text box, enter the t3 URL of the Administration Server for the WebLogic domain in the following format:

```
t3://hostname:port
```

In the **UserName** text box, enter the WebLogic Administrator user name.

In the **Password** text box, enter the WebLogic Administrator password.

After entering information in the fields, click **Next** to continue.

H.5 OIM Server

Use this screen to set a password for the for the system administrator (`xelsysadm`).

Figure H–5 OIM Server Screen

Table H–3 describes the Oracle Identity Manager Server parameters that you can configure.

Table H–3 Oracle Identity Manager Server Configuration Parameters

Field Name	Description
OIM Administrator Password	Enter a new password for the administrator. A valid password contains at least six characters, begins with an alphabetic character, and includes at least one number, one uppercase letter and one lowercase letter. The password cannot contain first name, last name, or login name of Oracle Identity Manager. Note that you are not prompted to enter this password in upgrade scenarios. You must set a password only if you are performing a new 11*g* installation.
Confirm Password	Enter the new password again to confirm.
OIM HTTP URL	Enter the http URL that front-ends the Oracle Identity Manager application. For example, `http://localhost:7002`. By default, this field contains the URL of the Oracle Identity Manager Managed Server.
KeyStore Password	Enter 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 Underscore (_), Dollar ($), Pound (#). The password must contain at least one number.
Confirm KeyStore Password	Enter the new password again to confirm.

After entering information in the fields, click **Next** to continue.

H.6 LDAP Sync and OAM

In this screen, you can perform the following optional tasks:

- Enable synchronization of Oracle Identity Manager roles, users, and their hierarchy to an LDAP directory
- Enable Identity Administration Integration with Oracle Access Manager (OAM)
- Configure Oracle Identity Manager to use Oracle BI Publisher by specifying the BI publisher URL

Figure H–6 LDAP Sync and OAM Screen

Enabling OIM-LDAP Synchronization

If you want to enable LDAP sync, you must first set up LDAP Sync for Oracle Identity Manager (OIM) before selecting the **Enable LDAP Sync** option on this screen. For information about setting up OIM-LDAP Sync, see Setting Up LDAP Synchronization. After setting up LDAP Synchronization, select the **Enable LDAP Sync** option.

If you do not want to perform the other optional tasks, click **Next** to continue.

Enabling Identity Administration Integration with Oracle Access Manager (OAM)

You must set up integration between OIM and OAM before enabling identity administration integration with OAM on this screen. For information about setting up the integration, see the chapter Integration Between OIM and OAM. After setting up the integration, select the **Enable Identity Administration Integration with OAM** option, and enter the following:

- **Password of Access Gate** - Enter the access gate password for Oracle Identity Manager. This is the same password you provided with the `oimAccessGatePwd` parameter for the `configureOIM` WLST command during the OIM-OAM integration setup.
- **Domain of Cookie** - Enter the domain in which Oracle Access Manager is installed. For example, `*.us.acme.com*`. This is the same cookie domain you provided with the `oimCookieDomain` parameter for the `configureOIM` WLST command during the OIM-OAM integration setup. Note that the period (.) at the beginning of the string is mandatory.

Note: When you choose to enable Identity Administration Integration with OAM, the LDAP synchronization for OIM is enabled, by default.

If you do not want to configure Oracle BI Publisher, click **Next** to continue.

Configuring Oracle Identity Manager to Use Oracle BI Publisher

Ensure that Oracle BI Publisher is installed on your local or remote machine.

To configure Oracle Identity Manager to use Oracle BI Publisher, select the **Configure BI Publisher** option, and enter the BI Publisher URL in the **BI Publisher URL** text box.

The URL is of the format: `http://hostname:port/xmlpserver`, where hostname and port are the host name and the port on which the Oracle BI Publisher server is running.

After entering information in the fields, click **Next** to continue.

H.7 LDAP Server

This screen is displayed only if you select the **Enable LDAP Sync** option on the LDAP Sync and OAM screen. In the LDAP Server screen, you should specify the authentication information for the Oracle Virtual Directory server, as you want to synchronize Oracle Identity Manager roles, users, and their hierarchy to an LDAP directory.

Figure H–7 LDAP Server Screen

Table H–4 describes the Oracle Virtual Directory Server parameters that you must specify.

Table H–4 LDAP Server Information

Field Name	Description
LDAP URL	Enter the LDAP URL in the format: `ldap://ovd_host:ovd_port`

Table H–4 (Cont.) LDAP Server Information

Field Name	Description
LDAP User	Enter the user name for the Oracle Virtual Directory administrator.
LDAP Password	Enter the password for the Oracle Virtual Directory administrator.
LDAP SearchDN	Enter the Distinguished Names (DN). For example, `dc=acme`, `dc=com` This is the top-level container for users and roles in LDAP that is used for Oracle Identity Manager for reconciliation purposes.

After entering information in the fields, click **Next** to continue.

H.8 LDAP Server Continued

This screen is a continuation of the LDAP Server screen.

Figure H–8 LDAP Server Continued Screen

Table H–5 describes the LDAP parameters that you must specify.

Table H–5 LDAP Server Continued Information

Field Name	Description
LDAP RoleContainer	Enter a name for the container that will be used as a default container of roles in the LDAP directory.
LDAP RoleContainer Description	Type a description for the role container.
LDAP UserContainer	Enter a name for the container that will be used as a default container of users in the LDAP directory.
LDAP UserContainer Description	Type a description for the user container.

Table H–5 (Cont.) LDAP Server Continued Information

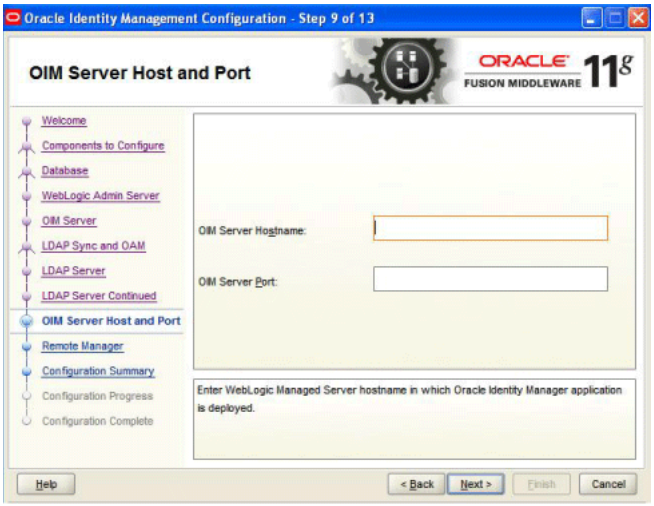
Field Name	Description
User Reservation Container	Enter a name for the container that will be used for reserving user names in the LDAP directory while their creation is being approved in Oracle Identity Manager. When the user names are approved, they are moved from the reservation container to the user container in the LDAP directory.

After entering information in the fields, click **Next** to continue.

H.9 OIM Server Host and Port

This screen is displayed only if you choose to configure Oracle Identity Manager Design Console on the Components to Configure screen, on Windows operating systems. Note that you must configure Oracle Identity Manager (OIM) Server on a local machine or a remote machine before running Design Console. In the OIM Server Host and Port screen, you must specify the host name and port information for the Oracle Identity Manager Server.

Figure H–9 OIM Server Host and Port Screen



In the **OIM Server Hostname** text box, enter the host name of the Oracle Identity Manager Managed Server that you configured during while configuring OIM in a new or existing WebLogic domain.

In the **OIM Server Port** text box, enter the port number for the Oracle Identity Manager Managed Server. This port is the Listen port you or your administrator specified while configuring OIM in a new or existing WebLogic administration domain.

After entering information in the fields, click **Next** to continue.

H.10 Remote Manager

Use this screen to configure the Oracle Identity Manager Remote Manager. Note that you must configure Oracle Identity Manager Server on the local machine or a remote machine before running Remote Manager.

Figure H–10 Remote Manager Screen

Table H–6 describes the Oracle Identity Manager Remote Manager parameters that you can configure.

Table H–6 Remote Manager Configuration

Field Name	Description
Service Name	Enter the service name for the Remote Manager.
RMI Registry Port	Enter the port number on which RMI registry should be started. The default value is 12345.
Listen Port (SSL)	Enter the SSL port number. On this port number, a secure socket is opened to listen to client requests. The default value is 12346.

After entering information in the fields, click **Next** to continue.

H.11 KeyStore Password

This screen is displayed if you choose to configure only Remote Manager on a remote machine (a machine where Oracle Identity Manager Server is not configured).

Figure H–11 KeyStore Password Screen

Table H–7 describes the keystore password requirements.

Table H–7 Fields in the KeyStore Password Screen

Field Name	Description
KeyStore Password	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 Underscore (_), Dollar ($), Pound (#). The password must contain at least one number.
Confirm KeyStore Password	Enter the new password again to confirm.

After entering information in the fields, click **Next** to continue.

H.12 Configuration Summary

This screen displays a list of the applications or components you have selected for configuration. It includes the following information:

- Location of your installation
- Disk space that will be used for the installation
- Applications or components you have selected for configuration
- Configuration choices you made on different screens in the Oracle Identity Manager Configuration Wizard

Figure H–12 Configuration Summary Screen

Review this summary screen.

Additionally, you can select to create a response file from your installation selections by clicking on the **Save** button in the Save Response File field. A response file can be used for silent or non-interactive installations of software requiring no or very little user input.

Click **Configure** to start configuring the selected Oracle Identity Manager components.

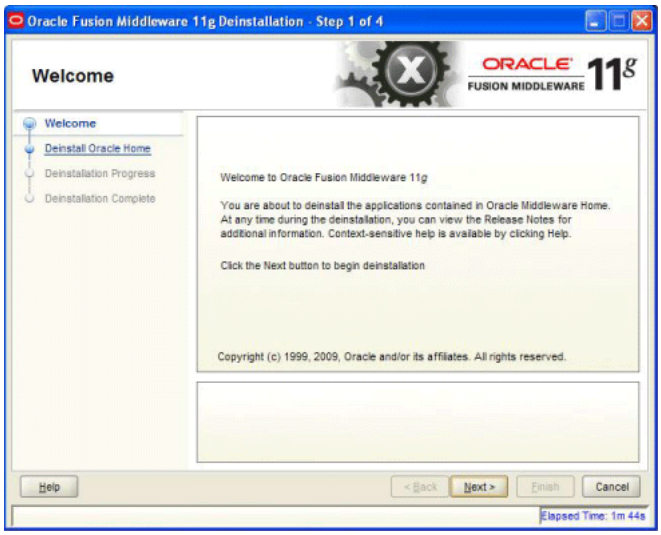
Software Deinstallation Screens

This appendix describes the screens of the Oracle Fusion Middleware 11*g* Deinstallation Wizard that enables you to remove the Oracle Identity Management software from your machine. This appendix contains the following topics:

I.1 Welcome

This screen is displayed each time you start the Oracle Fusion Middleware 11*g* Deinstallation Wizard.

Figure I–1 Deinstallation Welcome Screen

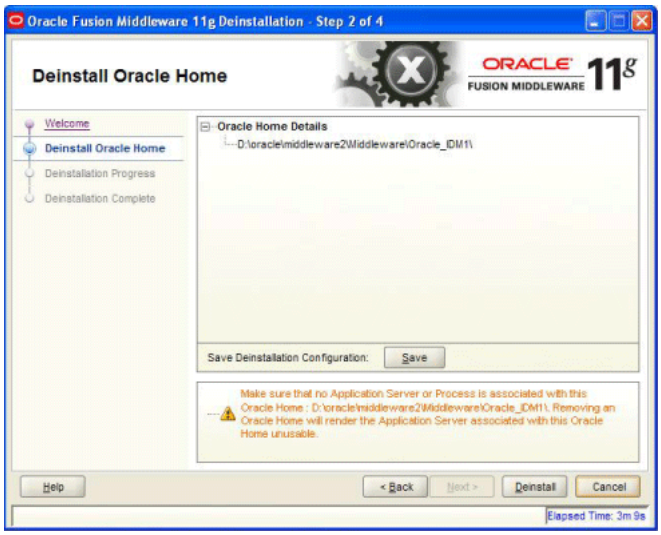


Click **Next** to continue.

I.2 Deinstall Oracle Home

This screen shows the Oracle Home directory that is about to be deinstalled. It is the Oracle Home directory in which the deinstaller was started.

Figure I–2 Deinstall Oracle Home Screen



Verify that this is the correct directory, and also verify that there are no processes associated with this Oracle Home.

Click **Deinstall** to start the deinstallation process.