Oracle® Fusion Middleware

Installation Guide for Oracle Identity and Access Management

11*g* Release 2 (11.1.2.2.0)

E49521-04

June 2014

This guide explains how to install and configure Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0) components.

ORACLE

Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management, 11*g* Release 2 (11.1.2.2.0)

E49521-04

Primary Author: Nisha Singh

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

Contents

Preface xiii

Audience xiii
Documentation Accessibility xiii
Related Documents xiv
Conventions xiv

Part I Introduction and Preparation

1 Introduction

1.1 Overview of Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0) 1-1
1.2 Additional 11*g* Release 2 (11.1.2.2.0) Deployment Information 1-1
1.2.1 Upgrading to Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0) 1-2
1.2.2 Migrating to Oracle Identity and Access Management 11g Release 2 (11.1.2.2.0) 1-2
1.2.3 Installing Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0) for High Availability 1-2
1.2.4 Deploying Oracle Unified Directory with Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0) 1-2
1.2.5 Installing Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0) on IBM WebSphere 1-3
1.3 Silent Installation 1-3
1.4 Understanding the State of Oracle Identity and Access Management Components After Installation 1-3
1.4.1 Default SSL Configurations 1-3
1.4.2 Default Passwords 1-3
1.5 Using This Guide 1-4

2 Preparing to Install

2.1 Reviewing System Requirements and Certification 2-1
2.2 Installing and Configuring Java Access Bridge (Windows Only) 2-1
2.3 Identifying Installation Directories 2-2
2.3.1 Oracle Middleware Home Location 2-2
2.3.2 Oracle Home Directory 2-2
2.3.3 Oracle Common Directory 2-3
2.3.4 Oracle WebLogic Domain Directory 2-3
2.3.5 WebLogic Server Directory 2-3

2.4 Determining Port Numbers 2-3
2.5 Locating Installation Log Files 2-3

Part II Installing and Configuring Oracle Identity and Access Management (11.1.2.2.0)

3 Installing and Configuring Oracle Identity and Access Management (11.1.2.2.0)

3.1 Installation and Configuration Roadmap 3-1
3.2 Installing and Configuring Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0) 3-2
3.2.1 Obtaining the Oracle Fusion Middleware Software 3-3
3.2.2 Database Requirements 3-3
3.2.2.1 Oracle Database Patch Requirements for Oracle Identity Manager 3-3
3.2.3 Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU) 3-4
3.2.4 WebLogic Server and Middleware Home Requirements 3-6
3.2.5 Installing Oracle SOA Suite (Oracle Identity Manager Users Only) 3-6
3.2.6 Starting the Oracle Identity and Access Management Installer 3-7
3.2.7 Installing Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0) 3-7
3.2.7.1 Products Installed 3-8
3.2.7.2 Dependencies 3-9
3.2.7.3 Procedure 3-9
3.2.7.4 Understanding the Directory Structure After Installation 3-11
3.2.8 Configuring Oracle Identity and Access Management (11.1.2.2.0) Products 3-11
3.2.9 Upgrading OPSS Schema using Patch Set Assistant 3-12
3.2.9.1 Starting Patch Set Assistant 3-12
3.2.9.2 Using the Patch Set Assistant Graphical Interface 3-13
3.2.9.3 Verifying Schema Upgrade 3-13
3.2.10 Configuring Database Security Store for an Oracle Identity and Access Management Domain 3-14
3.2.10.1 Overview 3-14
3.2.10.2 Before Configuring Database Security Store 3-15
3.2.10.3 Configuring the Database Security Store 3-16
3.2.10.4 Example Scenarios for Configuring the Database Security Store 3-18
3.2.11 Configuring Oracle Identity Manager Server, Design Console, and Remote Manager 3-20
3.2.12 Starting the Servers 3-21

4 Configuring Oracle Identity Navigator

4.1 Important Note Before You Begin 4-1
4.2 Installation and Configuration Roadmap for Oracle Identity Navigator 4-1
4.3 Configuring Oracle Identity Navigator in a New WebLogic Domain 4-2
4.3.1 Appropriate Deployment Environment 4-2
4.3.2 Components Deployed 4-3
4.3.3 Dependencies 4-3
4.3.4 Procedure 4-3

4.4 Starting the Servers 4-5
4.5 Verifying Oracle Identity Navigator 4-5
4.6 Getting Started with Oracle Identity Navigator After Installation 4-6

5 Configuring Oracle Identity Manager

5.1 Important Notes Before You Start Configuring Oracle Identity Manager 5-1
5.2 Installation and Configuration Roadmap for Oracle Identity Manager 5-2
5.3 Creating a new WebLogic Domain for Oracle Identity Manager and SOA 5-4
5.3.1 Appropriate Deployment Environment 5-4
5.3.2 Components Deployed 5-4
5.3.3 Dependencies 5-4
5.3.4 Procedure 5-5
5.4 Upgrading Oracle Platform Security Services Schema 5-8
5.5 Configuring Database Security Store 5-8
5.6 Starting the Servers 5-8
5.7 Overview of Oracle Identity Manager Configuration 5-8
5.7.1 Before Configuring Oracle Identity Manager Server, Design Console, or Remote Manager 5-9
5.7.1.1 Prerequisites for Configuring Oracle Identity Manager Server 5-9
5.7.1.2 Prerequisites for Configuring Only Oracle Identity Manager Design Console on a Different Machine 5-10
5.7.1.3 Prerequisites for Configuring Only Oracle Identity Manager Remote Manager on a Different Machine 5-10
5.7.2 Oracle Identity Manager Configuration Scenarios 5-10
5.7.2.1 Scope of Configuration Using the Oracle Identity Manager 11*g* Configuration Wizard 5-11
5.7.2.2 Scenario 1: Oracle Identity Manager Server and Design Console on Different Machines 5-11
5.7.2.3 Scenario 2: Oracle Identity Manager Server and Remote Manager on Different Machines 5-12
5.7.2.4 Scenario 3: Oracle Identity Manager Server, Design Console, and Remote Manager on a Single Windows Machine 5-12
5.8 Starting the Oracle Identity Manager 11*g* Configuration Wizard 5-13
5.9 Configuring Oracle Identity Manager Server 5-13
5.9.1 Appropriate Deployment Environment 5-13
5.9.2 Components Deployed 5-13
5.9.3 Dependencies 5-14
5.9.4 Procedure 5-14
5.9.5 Completing the Prerequisites for Enabling LDAP Synchronization 5-18
5.9.5.1 Preconfiguring the Identity Store 5-18
5.9.5.2 Creating Adapters in Oracle Virtual Directory 5-24
5.9.6 Running the LDAP Post-Configuration Utility 5-40
5.9.7 Verifying the LDAP Synchronization 5-44
5.9.8 Post-Configuration Steps 5-44
5.9.9 Setting oamEnabled Parameter for Identity Virtualization Library 5-46
5.9.10 Enabling LDAP Sync after Installing and Configuring Oracle Identity Manager Server at a Later Point 5-47
5.10 Optional: Configuring Oracle Identity Manager Design Console 5-48

5.10.1 Appropriate Deployment Environment ... 5-48
5.10.2 Components Deployed ... 5-48
5.10.3 Dependencies ... 5-48
5.10.4 Procedure ... 5-48
5.10.5 Post-Configuration Steps ... 5-49
5.10.6 Updating the xlconfig.xml File to Change the Port for Design Console ... 5-50
5.10.7 Configuring Design Console to Use SSL ... 5-51
5.11 Optional: Configuring Oracle Identity Manager Remote Manager ... 5-52
5.11.1 Appropriate Deployment Environment ... 5-52
5.11.2 Components Deployed ... 5-52
5.11.3 Dependencies ... 5-52
5.11.4 Procedure ... 5-52
5.12 Verifying the Oracle Identity Manager Installation ... 5-53
5.13 Changing Memory Settings for Oracle Identity Manager ... 5-54
5.14 Setting Up Integration with Oracle Access Management ... 5-55
5.15 List of Supported Languages ... 5-55
5.16 Using the Diagnostic Dashboard ... 5-55
5.17 Getting Started with Oracle Identity Manager After Installation ... 5-55

6 Configuring Oracle Access Management

6.1 Overview ... 6-1
6.2 Important Note Before You Begin ... 6-1
6.3 Installation and Configuration Roadmap for Oracle Access Management ... 6-2
6.4 Optional: Enabling TDE in Database ... 6-3
6.5 Oracle Access Management in a New WebLogic Domain ... 6-4
6.5.1 Appropriate Deployment Environment ... 6-4
6.5.2 Components Deployed ... 6-4
6.5.3 Dependencies ... 6-4
6.5.4 Procedure ... 6-4
6.6 Starting the Servers ... 6-6
6.7 Optional Post-Installation Tasks ... 6-6
6.8 Verifying the Oracle Access Management Installation ... 6-7
6.9 Setting Up Oracle Access Manager Agents ... 6-7
6.10 Setting Up Integration with OIM ... 6-7
6.11 Getting Started with Oracle Access Management After Installation ... 6-7

7 Configuring Oracle Adaptive Access Manager

7.1 Overview ... 7-1
7.2 Important Note Before You Begin ... 7-1
7.3 Installation and Configuration Roadmap for Oracle Adaptive Access Manager ... 7-2
7.4 Oracle Adaptive Access Manager in a New WebLogic Domain ... 7-3
7.4.1 Appropriate Deployment Environment ... 7-3
7.4.2 Components Deployed ... 7-3
7.4.3 Dependencies ... 7-3
7.4.4 Procedure ... 7-4
7.5 Configuring Oracle Adaptive Access Manager (Offline) ... 7-6
7.5.1 Components Deployed ... 7-6

7.5.2 Dependencies ... 7-6
7.5.3 Procedure ... 7-6
7.6 Starting the Servers ... 7-8
7.7 Post-Installation Steps ... 7-8
7.8 Verifying the Oracle Adaptive Access Manager Installation ... 7-11
7.9 Getting Started with Oracle Adaptive Access Manager After Installation ... 7-11

8 Installing and Configuring Oracle Entitlements Server

8.1 Important Note Before You Begin ... 8-1
8.2 Overview of Oracle Entitlements Server 11*g* Installation ... 8-1
8.3 Installation and Configuration Roadmap for Oracle Entitlements Server ... 8-2
8.4 Configuring Oracle Entitlements Server Administration Server ... 8-3
8.4.1 Components Deployed ... 8-3
8.4.2 Extracting Apache Derby Template (Optional) ... 8-3
8.4.3 Configuring Oracle Entitlements Server in a New WebLogic Domain ... 8-3
8.4.4 Upgrading OPSS Schema using Patch Set Assistant ... 8-5
8.4.4.1 Starting Patch Set Assistant ... 8-6
8.4.4.2 Using the Patch Set Assistant Graphical Interface ... 8-6
8.4.4.3 Verifying Schema Upgrade ... 8-6
8.4.5 Configuring Security Store for Oracle Entitlements Server Administration Server ... 8-7
8.4.6 Starting the Servers ... 8-9
8.4.7 Verifying Oracle Entitlements Server Configuration ... 8-9
8.5 Installing Oracle Entitlements Server Client ... 8-10
8.5.1 Prerequisites ... 8-10
8.5.2 Obtaining Oracle Entitlements Server Client Software ... 8-10
8.5.3 Installing Oracle Entitlements Server Client ... 8-10
8.5.4 Verifying Oracle Entitlements Server Client Installation ... 8-12
8.5.5 Applying a Patch Using OPatch ... 8-12
8.6 Configuring Oracle Entitlements Server Client ... 8-13
8.6.1 Configuring Distribution Modes ... 8-14
8.6.1.1 Configuring Controlled Push Distribution Mode ... 8-14
8.6.1.2 Configuring Non-Controlled and Controlled Pull Distribution Mode ... 8-14
8.6.2 Configuring Security Modules in a Controlled Push Mode (Quick Configuration) ... 8-17
8.6.2.1 Configuring Java Security Module in a Controlled Push Mode ... 8-17
8.6.2.2 Configuring RMI Security Module in a Controlled Push Mode ... 8-17
8.6.2.3 Configuring Web Service Security Module in a Controlled Push Mode ... 8-18
8.6.2.4 Configuring Oracle WebLogic Server Security Module in a Controlled Push Mode 8-18
8.6.3 Configuring Security Modules ... 8-18
8.6.3.1 Configuring WebLogic Server Security Module ... 8-19
8.6.3.2 Configuring Web Service Security Module ... 8-25
8.6.3.3 Configuring Web Service Security Module on Oracle WebLogic Server ... 8-26
8.6.3.4 Configuring Oracle Service Bus Security Module ... 8-33
8.6.3.5 Configuring IBM WebSphere Security Module ... 8-36
8.6.3.6 Configuring JBoss Security Module ... 8-36
8.6.3.7 Configuring the Apache Tomcat Security Module ... 8-37

8.6.3.8 Configuring Java Security Module 8-38
8.6.3.9 Configuring RMI Security Module 8-39
8.6.3.10 Configuring Microsoft .NET Security Module 8-39
8.6.3.11 Configuring Microsoft SharePoint Server (MOSS) Security Module 8-42
8.6.4 Locating Security Module Instances 8-46
8.6.5 Using the Java Security Module 8-46
8.6.6 Configuring the PDP Proxy Client 8-47
8.7 Getting Started with Oracle Entitlements Server After Installation 8-47

9 Configuring Oracle Privileged Account Manager

9.1 Overview 9-1
9.2 Important Note Before You Begin 9-1
9.3 Installation and Configuration Roadmap for Oracle Privileged Account Manager 9-2
9.4 Optional: Enabling TDE in Oracle Privileged Account Manager Data Store 9-3
9.4.1 Enabling TDE in the Database 9-3
9.4.2 Enabling Encryption in OPAM Schema 9-3
9.5 Configuring Oracle Privileged Account Manager and Oracle Identity Navigator in a New WebLogic Domain 9-4
9.5.1 Deployment Environment 9-4
9.5.2 Components Deployed 9-4
9.5.3 Dependencies 9-4
9.5.4 Procedure 9-4
9.6 Starting the Oracle WebLogic Administration Server 9-6
9.7 Post-Installation Tasks 9-6
9.8 Starting the Managed Server 9-8
9.9 Assigning the Application Configurator Role to a User 9-8
9.10 Optional: Setting Up Non-TDE Mode 9-8
9.11 Optional: Configuring OPAM Console 9-9
9.12 Verifying Oracle Privileged Account Manager 9-9
9.13 Getting Started with Oracle Privileged Account Manager After Installation 9-10

10 Configuring Oracle Access Management Mobile and Social

10.1 Overview 10-1
10.2 Important Note Before You Begin 10-1
10.3 Installation and Configuration Roadmap for Oracle Access Management Mobile and Social 10-1
10.4 Configuring Oracle Access Management Mobile and Social with Oracle Access Manager 10-3
10.4.1 Overview 10-3
10.4.2 Appropriate Deployment Environment 10-3
10.4.3 Components Deployed 10-3
10.4.4 Dependencies 10-3
10.4.5 Procedure 10-4
10.5 Verifying Oracle Access Management Mobile and Social 10-6
10.6 Getting Started with Oracle Access Management Mobile and Social After Installation 10-6

11 Lifecycle Management

11.1 How Lifecycle Events Impact Integrated Components 11-1
11.2 LCM for Oracle Identity Manager 11-1
11.3 LCM for Oracle Access Manager 11-2
11.4 LCM for Oracle Adaptive Access Manager 11-2
11.5 LCM for Oracle Identity Navigator 11-3
11.6 References 11-3

Part III Appendixes

A Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0) Software Installation Screens

A.1 Welcome A-1
A.2 Install Software Updates A-2
A.3 Prerequisite Checks A-3
A.4 Specify Installation Location A-4
A.5 Installation Summary A-6
A.6 Installation Progress A-6
A.7 Installation Complete A-7

B Oracle Identity Manager Configuration Screens

B.1 Welcome B-1
B.2 Components to Configure B-3
B.3 Database B-4
B.4 WebLogic Admin Server B-5
B.5 OIM Server B-6
B.6 LDAP Server B-8
B.7 LDAP Server Continued B-9
B.8 Configuration Summary B-10

C Starting or Stopping the Oracle Stack

C.1 Starting the Stack C-1
C.2 Stopping the Stack C-4
C.3 Restarting Servers C-4

D Preconfiguring Oracle Directory Server Enterprise Edition (ODSEE)

E Preconfiguring Oracle Unified Directory (OUD)

F Preconfiguring Oracle Internet Directory (OID)

G Preconfiguring Active Directory

H Creating Oracle Entitlement Server Schemas for Apache Derby

I Configuring the PDP Proxy Client for Web Service Security Module

J Deinstalling and Reinstalling Oracle Identity and Access Management

J.1 Deinstalling Oracle Identity and Access Management J-1
J.1.1 Deinstalling the Oracle Identity and Access Management Oracle Home J-1
J.1.2 Deinstalling the Oracle Common Home J-2
J.2 Reinstalling Oracle Identity and Access Management J-3

K Troubleshooting the Installation

K.1 General Troubleshooting Tips K-1
K.2 Installation Log Files K-2
K.3 Configuring OIM Against an Existing OIM 11*g* Schema K-2
K.4 Need More Help? K-3

L Oracle Adaptive Access Manager Partition Schema Reference

L.1 Overview L-1
L.2 Partition Add Maintenance L-2
L.2.1 .....Sp_Oaam_Add_Monthly_Partition L-2
L.2.2 .....Sp_Oaam_Add_Weekly_Partition L-2
L.3 Partition Maintenance Scripts L-3
L.3.1 drop_monthly_partition_tables.sql L-3
L.3.2 drop_weekly_partition_tables.sql L-3
L.3.3 add_monthly_partition_tables.sql L-3
L.3.4 add_weekly_partition_tables.sql L-3

M Software Deinstallation Screens

M.1 Welcome M-1
M.2 Select Deinstallation Type M-2
M.2.1 Option 1: Deinstall Oracle Home M-2
M.2.1.1 Deinstall Oracle Home M-3
M.2.2 Option 2: Deinstall ASInstances managed by WebLogic Domain M-3
M.2.2.1 Specify WebLogic Domain Detail M-3
M.2.2.2 Select Managed Instance M-4
M.2.2.3 Deinstallation Summary (Managed Instance) M-5
M.2.3 Option 3: Deinstall Unmanaged ASInstances M-6

M.2.3.1 Specify Instance Location M-6
M.2.3.2 Deinstallation Summary (Unmanaged ASInstance) M-6
M.3 Deinstallation Progress M-7
M.4 Deinstallation Complete M-8

Preface

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

- Audience
- Documentation Accessibility
- Related Documents
- Conventions

Audience

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

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

For information on installing Oracle Identity and Access Management components on IBM WebSphere, refer to *Oracle Fusion Middleware Third-Party Application Server Guide for Oracle Identity and Access Management*.

Documentation Accessibility

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

Access to Oracle Support

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

Related Documents

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

http://docs.oracle.com/

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

Oracle Fusion Middleware

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

High Availability

Oracle Fusion Middleware High Availability Guide

Oracle Fusion Middleware Repository Creation Utility

Oracle Fusion Middleware Repository Creation Utility User's Guide

Oracle Identity Manager

Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager

Oracle Access Management

Oracle Fusion Middleware Administrator's Guide for Oracle Access Management

Oracle Adaptive Access Manager

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

Oracle Identity Navigator

Oracle Fusion Middleware Administrator's Guide for Oracle Identity Navigator

Oracle Privileged Account Manager

Oracle Fusion Middleware Administrator's Guide for Oracle Privileged Account Manager

Oracle Access Management Mobile and Social

Oracle Fusion Middleware Administrator's Guide for Oracle Access Management

Oracle Entitlements Server

Oracle Fusion Middleware Administrator's Guide for Oracle Entitlements Server

Third-Party Application Server Guide for Oracle Identity and Access Management

Oracle Fusion Middleware Third-Party Application Server Guide for Oracle Identity and Access Management

Conventions

The following text conventions are used in this document:

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

Part I

Introduction and Preparation

Part I introduces Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0) installation and describes how to perform preparatory tasks. It contains the following chapters:

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

1 Introduction

This chapter provides an overview of Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0). This chapter includes the following topics:

- Overview of Oracle Identity and Access Management 11g Release 2 (11.1.2.2.0)
- Additional 11g Release 2 (11.1.2.2.0) Deployment Information
- Silent Installation
- Understanding the State of Oracle Identity and Access Management Components After Installation
- Using This Guide

1.1 Overview of Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0)

Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0) includes the following components:

- Oracle Identity Manager
- Oracle Access Management
- Oracle Identity Navigator
- Oracle Adaptive Access Manager
- Oracle Entitlements Server
- Oracle Privileged Account Manager
- Oracle Access Management Mobile and Social

> **Note:** Oracle Unified Directory 11*g* Release 2 installation is not covered in this guide.
>
> For information on installing Oracle Unified Directory 11*g* Release 2, see the *Oracle Unified Directory Installation Guide*.

1.2 Additional 11*g* Release 2 (11.1.2.2.0) Deployment Information

This topic describes additional sources for 11*g* Release 2 (11.1.2.2.0) deployment information, including documentation on the following subjects:

- Upgrading to Oracle Identity and Access Management 11g Release 2 (11.1.2.2.0)

- Migrating to Oracle Identity and Access Management 11g Release 2 (11.1.2.2.0)
- Installing Oracle Identity and Access Management 11g Release 2 (11.1.2.2.0) for High Availability
- Deploying Oracle Unified Directory with Oracle Identity and Access Management 11g Release 2 (11.1.2.2.0)
- Installing Oracle Identity and Access Management 11g Release 2 (11.1.2.2.0) on IBM WebSphere

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

1.2.1 Upgrading to Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0)

This guide does not explain how to upgrade previous versions of Oracle Identity and Access Management components, including any previous database schemas, to 11*g* Release 2 (11.1.2.2.0). To upgrade an Oracle Identity and Access Management component that is earlier than 11*g*, refer to *Oracle Fusion Middleware Upgrade and Migration Guide for Oracle Identity and Access Management*.

1.2.2 Migrating to Oracle Identity and Access Management 11g Release 2 (11.1.2.2.0)

This guide does not explain how to migrate to Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0) components. To migrate to an Oracle Identity and Access Management component, refer to *Oracle Fusion Middleware Migration Guide for Oracle Identity and Access Management*.

1.2.3 Installing Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0) for High Availability

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

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

1.2.4 Deploying Oracle Unified Directory with Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0)

Oracle Unified Directory (OUD) 11*g* Release 2 can be deployed in the following ways:

- Oracle Unified Directory 11*g* Release 2 in an Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0) domain.
- Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0) products in an Oracle Unified Directory 11*g* Release 2 domain.

Note: Oracle Unified Directory 11*g* Release 2 installation is not covered in this guide.

For information on installing Oracle Unified Directory 11*g* Release 2, see the *Oracle Unified Directory Installation Guide*.

1.2.5 Installing Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0) on IBM WebSphere

This guide does not explain how to install Oracle Identity and Access Management on IBM WebSphere. To install and configure Oracle Identity and Access Management components on IBM WebSphere, refer to *Oracle Fusion Middleware Third-Party Application Server Guide for Oracle Identity and Access Management*.

1.3 Silent Installation

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

For information on performing silent installation, refer to the "Silent Oracle Fusion Middleware Installation and Deinstallation" topic in the *Oracle Fusion Middleware Installation Planning Guide for Oracle Identity and Access Management*.

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

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

- Default SSL Configurations
- Default Passwords

1.4.1 Default SSL Configurations

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

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

1.4.2 Default Passwords

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

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

1.5 Using This Guide

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

1. Install single instances of Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0) components.
2. Verify the installation was successful.
3. Get started with the component after installation.

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

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

Part II of this guide explains how to install Oracle Identity Manager, Oracle Access Management, Oracle Adaptive Access Manager, Oracle Entitlements Server, Oracle Identity Navigator, Oracle Privileged Account Manager, and Oracle Access Management Mobile and Social, by using the Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0) Installer and the Oracle Fusion Middleware Configuration Wizard. The Oracle Identity Manager 11*g* Configuration Wizard is used for configuring Oracle Identity Manager only.

The following is a list of recommendations on how to use the information in this guide to install Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0):

1. Review Chapter 1, "Introduction," for context.
2. Review Chapter 2, "Preparing to Install," for information about what you should consider before you deploy Oracle Identity and Access Management.
3. Review Chapter 3, "Installing and Configuring Oracle Identity and Access Management (11.1.2.2.0)," for general installation and configuration information which applies to all Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0) products.
4. Install, configure, verify, and get started with your Oracle Identity and Access Management component by referring to its specific chapter in this guide.
5. Use the appendixes in this guide as needed.

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

2

Preparing to Install

This chapter provides information you should review before installing Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0).

This chapter discusses the following topics:

- Reviewing System Requirements and Certification
- Installing and Configuring Java Access Bridge (Windows Only)
- Identifying Installation Directories
- Determining Port Numbers
- Locating Installation Log Files

2.1 Reviewing System Requirements and Certification

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

- *Oracle Fusion Middleware System Requirements and Specifications*

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

- *Oracle Fusion Middleware Supported System Configurations*

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

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

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

2.2 Installing and Configuring Java Access Bridge (Windows Only)

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

1. Download Java Access Bridge from the following URL:

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

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

2.3 Identifying Installation Directories

This topic describes directories you must identify in most Oracle Identity and Access Management installations and configurations.

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

For more information about the common directories and basic concepts of Oracle Fusion Middleware and Oracle WebLogic Server, refer to "Understanding Oracle Fusion Middleware Concepts" in the *Oracle Fusion Middleware Administrator's Guide*.

2.3.1 Oracle Middleware Home Location

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

2.3.2 Oracle Home Directory

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

The Installer installs the files required to host the component, such as binaries and libraries, in the Oracle Home directory. In examples, the Oracle home path is identified with the *ORACLE_HOME* variable.

This directory is also referred to as *IAM_HOME* in this book.

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

2.3.3 Oracle Common Directory

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

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

2.3.4 Oracle WebLogic Domain Directory

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

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

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

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

2.3.5 WebLogic Server Directory

Enter the path to your Oracle WebLogic Server Home directory. This directory contains the files required to host the Oracle WebLogic Server. In examples, it is identified with the WL_HOME variable.

2.4 Determining Port Numbers

If you want to install an Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0) component against an existing Oracle Identity and Access Management component, you may need to identify the ports for the existing component. For example, if you want to install Oracle Identity Manager against an existing Oracle Internet Directory instance, then you must identify its port when you install Oracle Identity Manager.

2.5 Locating Installation Log Files

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

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

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

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

- install*DATE-TIME_STAMP*.log

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

Part II

Installing and Configuring Oracle Identity and Access Management (11.1.2.2.0)

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

- Oracle Identity Manager
- Oracle Access Management
- Oracle Adaptive Access Manager
- Oracle Entitlements Server
- Oracle Identity Navigator
- Oracle Privileged Account Manager
- Oracle Access Management Mobile and Social

Part II contains the following chapters:

- Chapter 3, "Installing and Configuring Oracle Identity and Access Management (11.1.2.2.0)"
- Chapter 4, "Configuring Oracle Identity Navigator"
- Chapter 5, "Configuring Oracle Identity Manager"
- Chapter 6, "Configuring Oracle Access Management"
- Chapter 7, "Configuring Oracle Adaptive Access Manager"
- Chapter 8, "Installing and Configuring Oracle Entitlements Server"
- Chapter 9, "Configuring Oracle Privileged Account Manager"
- Chapter 10, "Configuring Oracle Access Management Mobile and Social"
- Chapter 11, "Lifecycle Management"

3

Installing and Configuring Oracle Identity and Access Management (11.1.2.2.0)

This chapter includes the following topics:

- Installation and Configuration Roadmap
- Installing and Configuring Oracle Identity and Access Management 11g Release 2 (11.1.2.2.0)

3.1 Installation and Configuration Roadmap

Table 3–1 lists the general installation and configuration tasks that apply to Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0) products.

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

No.	Task	Description
1	Review installation concepts in the Installation Planning Guide.	Read the *Oracle Fusion Middleware Installation Planning Guide*, which describes the process for various users to install or upgrade to Oracle Fusion Middleware 11*g* (11.1.2) depending on the user's existing environment.
2	Review the system requirements and certification documents to ensure that your environment meets the minimum installation requirements for the components you are installing.	For more information, see Section 2.1, "Reviewing System Requirements and Certification".
3	Obtain the Oracle Fusion Middleware Software.	For more information, see Section 3.2.1, "Obtaining the Oracle Fusion Middleware Software"
4	Review the Database requirements.	For more information, see Section 3.2.2, "Database Requirements". **Note:** Some of the Oracle Database versions require patches. For more information, see Section 3.2.2.1, "Oracle Database Patch Requirements for Oracle Identity Manager".
5	Run Oracle Fusion Middleware Repository Creation Utility (RCU) to create and load the appropriate schemas for Oracle Identity and Access Management products.	For more information, see Section 3.2.3, "Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU)".
6	Review WebLogic Server and Middleware Home requirements.	For more information, see Section 3.2.4, "WebLogic Server and Middleware Home Requirements".

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

No.	Task	Description
7	For Oracle Identity Manager users only: Install Oracle SOA Suite 11*g* Release 1 (11.1.1.7.0).	For more information, see Section 3.2.5, "Installing Oracle SOA Suite (Oracle Identity Manager Users Only)". **Note:** After installing Oracle SOA Suite 11.1.1.7.0, you must apply mandatory SOA patches before installing Oracle Identity Manager. For more information, see "SOA Patch Requirements for Oracle Identity Manager".
8	Start the Oracle Identity and Access Management Installer.	For more information, see Section 3.2.6, "Starting the Oracle Identity and Access Management Installer".
9	Install the Oracle Identity and Access Management 11*g* software.	For more information, see Section 3.2.7, "Installing Oracle Identity and Access Management 11g Release 2 (11.1.2.2.0)".
10	Run the Oracle Fusion Middleware Configuration Wizard to configure your Oracle Identity and Access Management products in a new or existing WebLogic domain.	For more information, see Section 3.2.8, "Configuring Oracle Identity and Access Management (11.1.2.2.0) Products".
11	Upgrade the OPSS schema using Patch Set Assistant	For more information, see Section 3.2.9, "Upgrading OPSS Schema using Patch Set Assistant".
12	Configure the Database Security Store.	For more information, see Section 3.2.10, "Configuring Database Security Store for an Oracle Identity and Access Management Domain".
13	For Oracle Identity Manager users only: ▪ Configure the Oracle Identity Manager Server by running the Oracle Identity Manager configuration wizard. ▪ Optional: Configure Oracle Identity Manager Design Console. ▪ Optional: Configure Oracle Identity Manager Remote Manager.	For more information, see Section 3.2.11, "Configuring Oracle Identity Manager Server, Design Console, and Remote Manager".
14	Start the servers.	You must start the Administration Server and all Managed Servers. For more information, see Section C.1, "Starting the Stack".

3.2 Installing and Configuring Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0)

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

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

- Obtaining the Oracle Fusion Middleware Software
- Database Requirements
- Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU)
- WebLogic Server and Middleware Home Requirements
- Installing Oracle SOA Suite (Oracle Identity Manager Users Only)

- Starting the Oracle Identity and Access Management Installer
- Installing Oracle Identity and Access Management 11g Release 2 (11.1.2.2.0)
- Configuring Oracle Identity and Access Management (11.1.2.2.0) Products
- Upgrading OPSS Schema using Patch Set Assistant
- Configuring Database Security Store for an Oracle Identity and Access Management Domain
- Configuring Oracle Identity Manager Server, Design Console, and Remote Manager
- Starting the Servers

3.2.1 Obtaining the Oracle Fusion Middleware Software

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

- Oracle WebLogic Server 11*g* Release 1 (10.3.6)
- Oracle Database
- Oracle Repository Creation Utility
- Oracle Identity and Access Management Suite
- Oracle SOA Suite 11.1.1.7.0 (required for Oracle Identity Manager only)
- Oracle Entitlements Server Client (required for Oracle Entitlements Server only)

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

3.2.2 Database Requirements

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

Note: For information about certified databases, see the "Database Requirements" topic in the *Oracle Fusion Middleware System Requirements and Specifications for Oracle Identity and Access Management* 11*g* Release 2 (11.1.2) document.

For information about RCU requirements for Oracle Databases, see "RCU Requirements for Oracle Databases" in the *Oracle Fusion Middleware System Requirements and Specifications for Oracle Identity and Access Management* 11*g* Release 2 (11.1.2) document.

3.2.2.1 Oracle Database Patch Requirements for Oracle Identity Manager

Some of the Oracle Database versions require patches. To identify the patches required for Oracle Identity Manager 11.1.2 configurations that use Oracle Databases, refer to the "Oracle Identity Manager" section of the 11*g* Release 2 *Oracle Fusion Middleware Release Notes*.

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

You must create and load the appropriate Oracle Fusion Middleware schemas in the database using RCU before installing and configuring the following Oracle Identity and Access Management components:

- Oracle Identity Manager
- Oracle Access Management
- Oracle Adaptive Access Manager
- Oracle Entitlements Server
- Oracle Privileged Account Manager

Notes:

- To create database schemas for Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0) components, you must use the 11*g* Release 2 (11.1.2.2.0) version of the Oracle Fusion Middleware Repository Creation Utility.
- For information on RCU requirements, refer to the "Repository Creation Utility (RCU) Requirements" topic in the *Oracle Fusion Middleware System Requirements and Specifications for Oracle Identity and Access Management* 11*g* Release 2 (11.1.2) document.
- For general information about using RCU, use the *Oracle Fusion Middleware Repository Creation Utility User's Guide*. Ensure that the RCU version you are using matches the version number of the Oracle Fusion Middleware product you are installing.

  For information on creating schemas, see the "Creating Schemas" topic in the *Oracle Fusion Middleware Repository Creation Utility User's Guide*.
- This guide lists the schemas you must install for the Identity and Access Management software. For information about using RCU, this guide references the RCU documentation in a recent Oracle Fusion Middleware 11*g* Release 1 (11.1.1) documentation library.

  These general instructions for using RCU are valid, as long as you download and use the specific RCU version available as part of the Oracle Identity and Access Management 11*g* Release 2 (11.1.2) Media Pack on the Oracle Software Delivery Cloud.

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

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

- For Oracle Identity Manager, select the **Identity Management - Oracle Identity Manager** schema. When you select the **Identity Management - Oracle Identity Manager** schema, the following schemas are also selected, by default:
  - **SOA Infrastructure**
  - **User Messaging Service**

  - **AS Common Schemas - Oracle Platform Security Services**
  - **AS Common Schemas - Metadata Services**

- For Oracle Adaptive Access Manager, select the **Identity Management - Oracle Adaptive Access Manager** schema. When you select the Identity Management - Oracle Adaptive Access Manager schema, the following schemas are also selected, by default:
  - **AS Common Schemas - Oracle Platform Security Services**
  - **AS Common Schemas - Metadata Services**
  - **AS Common Schemas - Audit Services**

  For Oracle Adaptive Access Manager with partition schema support, select the **Identity Management - Oracle Adaptive Access Manager (Partition Supp...)** schema. When you select the **Identity Management - Oracle Adaptive Access Manager (Partition Supp...)** schema, the following schemas are also selected, by default:
  - **AS Common Schemas - Oracle Platform Security Services**
  - **AS Common Schemas - Metadata Services**
  - **AS Common Schemas - Audit Services**

  Note: For information about Oracle Adaptive Access Manager schema partitions, see Appendix L, "Oracle Adaptive Access Manager Partition Schema Reference".

- For Oracle Access Management, select the **Identity Management - Oracle Access Manager** schema. When you select the **Identity Management - Oracle Access Manager** schema, the following schemas are also selected, by default:
  - **AS Common Schemas - Oracle Platform Security Services**
  - **AS Common Schemas - Metadata Services**
  - **AS Common Schemas - Audit Services**

  Note: If you want to use Transparent Data Encryption (TDE) for Oracle Access Management, you must set up TDE for Oracle Access Management before creating the Oracle Access Management schema. For more information, see Section 6.4, "Optional: Enabling TDE in Database".

- For Oracle Entitlements Server, select the **AS Common Schemas - Oracle Platform Security Services** schema.
- For Oracle Privileged Account Manager, select the **Identity Management - Oracle Privileged Account Manager** schema. By default, the **AS Common Schemas - Oracle Platform Security Services** schema is also selected.

  Note: Oracle Privileged Account Manager schema must be created by a Database user with `SYSDBA` privileges.

Note: When you create a schema, be sure to remember the schema owner and password that is shown in RCU. You must specify the schema owner and password information when you configure the Oracle Identity and Access Management products.

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

3.2.4 WebLogic Server and Middleware Home Requirements

Before you install Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0) components, you must ensure that you have installed Oracle WebLogic Server, and created a Middleware Home directory.

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

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

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

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

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

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

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

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

SOA Patch Requirements for Oracle Identity Manager

After installing Oracle SOA Suite 11.1.1.7.0, you must apply mandatory SOA patches before installing Oracle Identity Manager. For information about the patches, refer to the "Mandatory Patches Required for Installing Oracle Identity Manager" topic in the 11*g* Release 2 *Oracle Fusion Middleware Release Notes*.

3.2.6 Starting the Oracle Identity and Access Management Installer

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

Start the Installer by executing one of the following commands:

On UNIX:

```
cd unpacked_archive_directory/Disk1
./runInstaller -jreLoc JRE_LOCATION
```

On Windows:

```
cd unpacked_archive_directory\Disk1
setup.exe -jreLoc JRE_LOCATION
```

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

```
<full path to the setup.exe directory>\setup.exe
-jreLoc C:\MW_HOME\jdk\jre
```

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

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

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

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

3.2.7 Installing Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0)

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

It includes the following sections:

- Products Installed

- Dependencies
- Procedure
- Understanding the Directory Structure After Installation

3.2.7.1 Products Installed

Performing the installation in this section installs the following products:

- Oracle Identity Manager
- Oracle Access Management

  Note: Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0) contains Oracle Access Management suite which includes the following services:

  - Oracle Access Manager
  - Oracle Access Management Security Token Service
  - Oracle Access Management Identity Federation
  - Oracle Access Management Mobile and Social
  - Identity Context

  For more information about these services, see "Understanding Oracle Access Management Services" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.

  For an introduction to the Oracle Access Management Mobile and Social, see "Understanding Mobile and Social" chapter in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.

- Oracle Adaptive Access Manager

  Note: For Oracle Identity and Access Management 11.1.2.2.0, Oracle Adaptive Access Manager includes two components

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

- Oracle Identity Navigator
- Oracle Entitlements Server

  Note: When you are installing Oracle Identity and Access Management, only the Administration Server of Oracle Entitlements Server is installed.

  To install and configure Oracle Entitlements Server Client, see Section 8.5, "Installing Oracle Entitlements Server Client".

- Oracle Privileged Account Manager

Note: For an introduction to the Oracle Privileged Account Manager, see "Understanding Oracle Privileged Account Manager" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Privileged Account Manager*.

3.2.7.2 Dependencies

The installation in this section depends on the following:

- Oracle WebLogic Server 11*g* Release 1 (10.3.6)
- Oracle Database and any required patches
- Oracle SOA Suite 11.1.1.7.0 (required for Oracle Identity Manager only)
- JDK (Java SE 6 Update 24 or higher) or JRockit

3.2.7.3 Procedure

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

1. Start your installation by performing all the steps in Section 3.2.6, "Starting the Oracle Identity and Access Management Installer". After you complete those steps, the Welcome screen appears.
2. Click **Next** on the Welcome screen. The Install Software Updates screen appears. Select whether or not you want to search for updates. Click **Next**.
3. The Prerequisite Checks screen appears. If all prerequisite checks pass inspection, click **Next**. The Specify Installation Location screen appears.
4. On the Specify Installation Location screen, enter the path to the Oracle Middleware Home that was created when you installed Oracle WebLogic Server 11*g* Release 1 (10.3.6) on your system.

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

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

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

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

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

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

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

6. The Installation Summary screen displays a summary of the choices that you made. Review this summary and decide whether to start the installation. If you want to modify any of the configuration settings at this stage, select a topic in the left navigation page and modify your choices.

   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.

   To continue installing Oracle Identity and Access Management, click **Install**.

7. The Installation Progress screen appears. 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**.

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

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

8. The Installation Complete screen appears. Click **Save** to save the installation summary file. This file contains information about the installation, 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.

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

   After installing the Oracle Identity and Access Management software, you must proceed to Section 3.2.8, "Configuring Oracle Identity and Access Management (11.1.2.2.0) Products," to configure Oracle Identity and Access Management products in a new or existing WebLogic domain.

3.2.7.4 Understanding the Directory Structure After Installation

This section describes the directory structure after installation of Oracle WebLogic Server and Oracle Identity and Access Management.

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

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

3.2.8 Configuring Oracle Identity and Access Management (11.1.2.2.0) Products

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

When you configure an Oracle Identity and Access Management 11.1.2.2.0 component, you can choose one of the following configuration options:

- Create a New Domain
- Extend an Existing Domain

> **Note:** You should not extend the Oracle Identity Management 11*g* Release 1 (11.1.1.6.0) domain to support Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0) products.

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

Start the Oracle Fusion Middleware Configuration Wizard by running the *`IAM_HOME`*`/common/bin/config.sh` script (on UNIX), or *`IAM_HOME`*`\common\bin\config.cmd` (on Windows).

Create a New Domain

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

Extend an Existing Domain

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

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

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

- Chapter 4, "Configuring Oracle Identity Navigator"
- Chapter 5, "Configuring Oracle Identity Manager"
- Chapter 6, "Configuring Oracle Access Management"
- Chapter 7, "Configuring Oracle Adaptive Access Manager"
- Chapter 8, "Installing and Configuring Oracle Entitlements Server,"
- Chapter 9, "Configuring Oracle Privileged Account Manager"
- Chapter 10, "Configuring Oracle Access Management Mobile and Social"

3.2.9 Upgrading OPSS Schema using Patch Set Assistant

After configuring the Oracle Identity and Access Management (11.1.2.2.0) components, you must upgrade the Oracle Platform Security Services (OPSS) schema that you had created using the RCU in Section 3.2.3, "Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU)".

To upgrade the schemas, complete the following steps:

- Starting Patch Set Assistant
- Using the Patch Set Assistant Graphical Interface
- Verifying Schema Upgrade

3.2.9.1 Starting Patch Set Assistant

To start Patch Set Assistant, do the following:

On UNIX:

1. Move from your present working directory to the *MW_HOME*`/oracle_common/bin` directory by running the following command on the command line:

   ```
   cd <MW_HOME>/oracle_common/bin
   ```

2. Run the following command:

   ```
   ./psa
   ```

On Windows:

1. Move from your present working directory to the *MW_HOME*`\oracle_common\bin` directory by running the following command on the command line:

   ```
   cd <MW_HOME>\oracle_common\bin
   ```

2. Execute the following command:

```
psa.bat
```

3.2.9.2 Using the Patch Set Assistant Graphical Interface

After starting the Patch Set Assistant Installer, follow the instructions in Table 3–2 to update your schemas.

Table 3–2 Patch Set Assistant Screens

Screen	Description
Welcome	This page introduces you to the Patch Set Assistant.
Select Component	In the Select Component screen, you must select only the **Oracle Platform Security Services** schema. **NOTE:** Do not select any other components that are listed on the Select Component screen.
Prerequisite	Verify that you have satisfied the database prerequisites.
Schema	Specify your database credentials to connect to your database, then select the schema you want to update. Note that this screen appears once for each schema that must be updated as a result of the component you selected on the Select Component screen.
Examine	This page displays the status of the Patch Set Assistant as it examines each component schema. Verify that your schemas have a "successful" indicator in the Status column.
Upgrade Summary	Verify that the schemas are the ones you want to upgrade.
Upgrade Progress	This screen shows the progress of the schema upgrade.
Upgrade Success	Once the upgrade is successful, this screen is displayed.

3.2.9.3 Verifying Schema Upgrade

You can verify the schema upgrade by checking out the log files. The Patch Set Assistant writes log files in the following locations:

On UNIX:

MW_HOME/oracle_common/upgrade/logs/psa/psatimestamp.log

On Windows:

MW_HOME\oracle_common\upgrade\logs\psa\psatimestamp.log

Some components create a second log file named `psatimestamp.out` in the same location.

The `timestamp` reflects the actual date and time when Patch Set Assistant was run.

If any failures occur when running Patch Set Assistant, you can use these log files to help diagnose and correct the problem. Do not delete them. You can alter the contents of the log files by specifying a different `-logLevel` from the command line.

Some of the operations performed by Patch Set Assistant may take longer to complete than others. If you want to see the progress of these long operations, you can see this information in the log file, or you can use the following query:

```
SELECT VERSION, STATUS, UPGRADED FROM SCHEMA_VERSION_REGISTRY WHERE OWNER='schema_
name';
```

In the query results, the STATUS field is either UPGRADING or UPGRADED during the schema patching operation, and becomes VALID when the operation is completed.

3.2.10 Configuring Database Security Store for an Oracle Identity and Access Management Domain

This section discusses the following topics:

- Overview
- Before Configuring Database Security Store
- Configuring the Database Security Store
- Example Scenarios for Configuring the Database Security Store

3.2.10.1 Overview

You must run the configureSecurityStore.py script to configure the Database Security Store as it is the only security store type supported by the Oracle Identity & Access Management 11*g* Release 2 (11.1.2.2.0).

The configureSecurityStore.py script is located in the *IAM_HOME*\common\tools directory. You can use the -h option for help information about using the script. Note that not all arguments will apply to configuring the Database Security Store.

For example:

On Windows:

```
<MW_HOME>\oracle_common\common\bin\wlst.cmd <IAM_
HOME>\common\tools\configureSecurityStore.py -h
```

On UNIX:

```
<MW_HOME>/oracle_common/common/bin/wlst.sh <IAM_
HOME>/common/tools/configureSecurityStore.py -h
```

Table 3–3 describes the parameters you that you may specify on the command line.

Table 3–3 Database Security Store Configuration Parameters

Parameter	Description
-d *domaindir*	Location of the directory containing the domain.
-m *mode*	create- Use create if you want to create a new database security store. join- Use join if you want to use an existing database security store for the domain. validate- Use validate to verify whether the Security Store has been configured correctly. This command validates diagnostics data created during initial creation of the Security Store. validate_fix- Use validate_fix to fix diagnostics data present in the Security Store. fixjse- Use fixjse to update the domain's Database Security Store credentials used for access by JSE tools.

Table 3–3 (Cont.) Database Security Store Configuration Parameters

Parameter	Description
`-c configmode`	The configuration mode of the domain. When configuring Database Security Store this value must be specified as `IAM`. **Special Instructions for OES Installation:** If you are an OES user, then the `-c` parameter is optional. In this case, the default value is `None`. **Note:** If `-c <config>` option is specified, OES Admin Server will be configured in mixed mode, then it can only distribute policies to Security Modules in non-controlled mode and controlled pull mode. For example: If the OES Administration Server is deployed in the domain where other Oracle Identity and Access Management components (OIM, OAM, OAAM, OPAM, or OIN) are deployed, then the domain is configured in mixed mode. In this case, the OES Administration Server is used for managing the Oracle Identity and Access Management policies only. It should not be used to manage the policies for any other applications protected by OES Security Modules. If `-c <config>` option is not specified, OES Admin Server will be configured in non-controlled mode, it can distribute policies to Security Modules in controlled push mode. For example: If you want to use OES Administration Server to manage custom applications which are protected by OES Security Modules, then the OES Administration Server must be deployed in a domain with non-controlled distribution mode.
`-p password`	The OPSS schema password.
`-k keyfilepath`	The directory containing the encryption key file `ewallet.p12`. If `-m join` is specified, this option is mandatory.
`-w keyfilepassword`	The password used when the domain's key file was generated. If `-m join` is specified, this option is mandatory.
`-u username`	The user name of the OPSS schema. If `-m fixjse` is specified, this option is mandatory.

3.2.10.2 Before Configuring Database Security Store

Each Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0) domain must be configured to have a Database Security Store. Before you configure the Database Security Store for an Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0) domain, you must identify the products to be configured in a single-domain scenario or in a multiple-domain scenario.

Note: Irrespective of the number of domains in a logical Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0) deployment (a logical deployment is a collection of Oracle Identity and Access Management products running in one or more domains and using a single database to hold product schemas), all domains share the same Database Security Store and use the same domain encryption key.

The Database Security Store is **created** at the time of creating the first domain, and then each new domain created is **joined** with the Database Security Store already created.

3.2.10.3 Configuring the Database Security Store

Following `configureSecurityStore.py` options are available for configuring the domain to use the Database Security Store:

- `-m create`
- `-m join`

Configuring the Database Security Store Using Create Option

To configure a domain to use a database security store using the `-m create` option, you must run the `configureSecurityStore.py` script as follows:

On Windows:

```
<MW_HOME>\oracle_common\common\bin\wlst.cmd <IAM_
HOME>\common\tools\configureSecurityStore.py -d <domaindir> -c IAM -p <opss_
schema_password> -m create
```

For example:

```
<MW_HOME>\oracle_common\common\bin\wlst.cmd <IAM_
HOME>\common\tools\configureSecurityStore.py -d <MW_Home>\user_
projects\domains\base_domain -c IAM -p welcome1 -m create
```

On UNIX:

```
<MW_HOME>/oracle_common/common/bin/wlst.sh <IAM_
HOME>/common/tools/configureSecurityStore.py -d <domaindir> -c IAM -p <opss_
schema_password> -m create
```

For example:

```
<MW_HOME>/oracle_common/common/bin/wlst.sh <IAM_
HOME>/common/tools/configureSecurityStore.py -d <MW_Home>/user_
projects/domains/base_domain -c IAM -p welcome1 -m create
```

Configuring the Database Security Store Using the Join Option

To configure a domain to use the database security store using the `-m join` option, you must first export the domain encryption key from a domain in the same logical Oracle Identity and Access Management deployment already configured to work with the database security store, and then run the `configureSecurityStore.py` script as follows:

Note: Exporting domain encryption key from a domain already configured to work with the Database Security Store is done via the WLST command:

```
exportEncryptionKey(jpsConfigFile=<jpsConfigFile>,keyFilePath=<keyF
ilePath>,keyFilePassword=<keyFilePassword>)
```

where:

`<jpsConfigFile>` - is the absolute location of the file `jps-config.xml` in the domain from which the encryption key is being exported.

`<keyFilePath>` - is the directory where the file `ewallet.p12` is created; note that the content of this file is encrypted and secured by `keyFilePassword`.

`<keyFilePassword>` - is the password to secure the file `ewallet.p12`; note that this same password must be used when importing that file.

On Windows:

1. Export encryption keys from a domain already configured to work with the Database Security Store as follows:

   ```
   <MW_HOME>\oracle_common\common\bin\wlst.cmd
   exportEncryptionKey(jpsConfigFile=<jpsConfigFile>, keyFilePath=<keyFilePath>,
   keyFilePassword=<keyFilePassword>)
   ```

2. Run the `configureSecurityStore.py` script with `-m join` option.

   ```
   <MW_HOME>\oracle_common\common\bin\wlst.cmd <IAM_
   HOME>\common\tools\configureSecurityStore.py -d <domaindir> -c IAM -p <opss_
   schema_password> -m join -k <keyfilepath> -w <keyfilepassword>
   ```

For example:

```
<MW_HOME>\oracle_common\common\bin\wlst.cmd
exportEncryptionKey(jpsConfigFile="<MW_HOME>\\user_projects\\domains\\base_
domain\\config\\fmwconfig\\jps-config.xml", keyFilePath="myDir\\key" ,
keyFilePassword="password")

<MW_HOME>\oracle_common\common\bin\wlst.cmd <IAM_
HOME>\common\tools\configureSecurityStore.py -d <MW_Home>\user_
projects\domains\base_domain1 -c IAM -p welcome1 -m join -k myDir -w password
```

On UNIX:

1. Export encryption keys from a domain already configured to work with the Database Security Store as follows:

   ```
   <MW_HOME>/oracle_common/common/bin/wlst.cmd
   exportEncryptionKey(jpsConfigFile=<jpsConfigFile>, keyFilePath=<keyFilePath>,
   keyFilePassword=<keyFilePassword>)
   ```

2. Run the `configureSecurityStore.py` script with `-m join` option.

   ```
   <MW_HOME>/oracle_common/common/bin/wlst.cmd <IAM_
   HOME>/common/tools/configureSecurityStore.py -d <domaindir> -c IAM -p <opss_
   schema_password> -m join -k <keyfilepath> -w <keyfilepassword>
   ```

For example:

```
<MW_HOME>/oracle_common/common/bin/wlst.cmd
exportEncryptionKey(jpsConfigFile="<MW_HOME>/user_projects/domains/base_
domain/config/fmwconfig/jps-config.xml", keyFilePath="myDir" ,
keyFilePassword="password")

<MW_HOME>/oracle_common/common/bin/wlst.cmd <IAM_
HOME>/common/tools/configureSecurityStore.py -d <MW_Home>/user_
projects/domains/base_domain1 -c IAM -p welcome1 -m join -k myDir -w password
```

Validating the Database Security Store Configuration

To validate whether the security store has been created or joined correctly, run the `configureSecurityStore.py` script with `-m validate` option, as follows:

On Windows:

```
<MW_HOME>\oracle_common\common\bin\wlst.cmd <IAM_
HOME>\common\tools\configureSecurityStore.py -d <domaindir> -m validate
```

For example:

```
<MW_HOME>\oracle_common\common\bin\wlst.cmd <IAM_
HOME>\common\tools\configureSecurityStore.py -d <MW_Home>\user_
projects\domains\base_domain -m validate
```

On UNIX:

```
<MW_HOME>/oracle_common/common/bin/wlst.sh <IAM_
HOME>/common/tools/configureSecurityStore.py -d <domaindir> -m validate
```

For example:

```
<MW_HOME>/oracle_common/common/bin/wlst.sh <IAM_
HOME>/common/tools/configureSecurityStore.py -d <MW_Home>/user_
projects/domains/base_domain -m validate
```

3.2.10.4 Example Scenarios for Configuring the Database Security Store

Consider the following example scenarios:

- Example Scenario for One or More Oracle Identity and Access Management Products in the Same Domain
- Example Scenario for Oracle Identity and Access Management Products in Different Domains

3.2.10.4.1 Example Scenario for One or More Oracle Identity and Access Management Products in the Same Domain

> **Note:** In a single-domain scenario, the command to create the Database Security Store is executed once after the domain is created but before the domain is started for the first time.

Scenario 1: Oracle Identity Manager, Oracle Access Management, and Oracle Adaptive Access Manager in the same WebLogic Administration Domain Sharing the same Database Security Store

To achieve this, you must complete the following tasks:

1. Create a new WebLogic domain for Oracle Identity Manager and SOA (for example, *oim_dom*) by completing the steps described in Table 5–1, " Installation and Configuration Flow for Oracle Identity Manager".

   After creating a new WebLogic domain for Oracle Identity Manager and SOA, run the `configureSecurityStore.py` script to configure the Database Security Store as follows:

   On Windows:

   ```
   <MW_HOME>\oracle_common\common\bin\wlst.cmd <IAM_
   HOME>\common\tools\configureSecurityStore.py -d <MW_Home>\user_
   projects\domains\oim_dom -c IAM -p welcome1 -m create
   ```

   On UNIX:

   ```
   <MW_HOME>/oracle_common/common/bin/wlst.sh <IAM_
   HOME>/common/tools/configureSecurityStore.py -d <MW_Home>/user_
   projects/domains/oim_dom -c IAM -p welcome1 -m create
   ```

2. Extend the Oracle Identity Manager domain (*oim_dom*) to include Oracle Access Management and Oracle Adaptive Access Manager. For more information, see "Extend an Existing Domain".

   Oracle Access Management and Oracle Adaptive Access Manager are added to the Oracle Identity Manager domain (*oim_dom*), and they share the same Database Security Store used by the Oracle Identity Manager domain.

3.2.10.4.2 Example Scenario for Oracle Identity and Access Management Products in Different Domains

---

Note: In a multiple-domain scenario, the command to create the Database Security Store is executed once after the first domain is created but before the domain is started for the first time.

For each subsequent domain, the command to join the existing Database Security Store is executed once after the domain is created but before the domain is started for the first time.

- **Scenario 1: Oracle Identity Manager and Oracle Access Management in different WebLogic Administration Domains Sharing the same Database Security Store**

  To achieve this, you must complete the following tasks:

  1. Create a new WebLogic domain for Oracle Identity Manager and SOA (for example, *oim_dom*) by completing the steps described in Table 5–1, " Installation and Configuration Flow for Oracle Identity Manager".

     After creating a new WebLogic domain for Oracle Identity Manager and SOA, run the `configureSecurityStore.py` script to configure the Database Security Store as follows:

     On Windows:

     ```
     <MW_HOME>\oracle_common\common\bin\wlst.cmd <IAM_
     HOME>\common\tools\configureSecurityStore.py -d <MW_Home>\user_
     projects\domains\oim_dom -c IAM -p welcome1 -m create
     ```

     On UNIX:

```
<MW_HOME>/oracle_common/common/bin/wlst.sh <IAM_
HOME>/common/tools/configureSecurityStore.py -d <MW_Home>/user_
projects/domains/oim_dom -c IAM -p welcome1 -m create
```

2. Create a new WebLogic domain for Oracle Access Management (for example *oam_dom*) by completing the steps described in Table 6–1, " Installation and Configuration Flow for Oracle Access Management".

   After creating a new WebLogic domain for Oracle Access Management, export the domain encryption key from the Oracle Identity Manager/SOA domain, and run the `configureSecurityStore.py` script to configure the Database Security Store as follows:

   On Windows:

```
<MW_HOME>\oracle_common\common\bin\wlst.cmd
exportEncryptionKey(jpsConfigFile="<MW_Home>\\user_projects\\domains\\oim_
dom\\config\\fmwconfig\\jps-config.xml", keyFilePath="myDir"
,keyFilePassword="password")

<MW_HOME>\oracle_common\common\bin\wlst.cmd <IAM_
HOME>\common\tools\configureSecurityStore.py -d <MW_Home>\user_
projects\domains\oam_dom -c IAM -p welcome1 -m join -k myDir -w password
```

   On UNIX:

```
<MW_HOME>/oracle_common/common/bin/wlst.sh
exportEncryptionKey(jpsConfigFile="<MW_Home>/user_projects/domains/oim_
dom/config/fmwconfig/jps-config.xml", keyFilePath="myDir"
,keyFilePassword="password")

<MW_HOME>/oracle_common/common/bin/wlst.sh <IAM_
HOME>/common/tools/configureSecurityStore.py -d <MW_Home>/user_
projects/domains/oam_dom -c IAM -p welcome1 -m join -k myDir -w password
```

- **Scenario 2: Extend the Oracle Access Management Domain previously joined to the Database Security Store to include Oracle Adaptive Access Manager**

  To achieve this, extend the Oracle Access Management domain (*oam_dom*) to include Oracle Adaptive Access Manager. For more information, see "Extend an Existing Domain".

  Oracle Adaptive Access Manager is added to the Oracle Access Management domain (*oam_dom*), and they both share the same Database Security Store used by the Oracle Access Manager domain.

3.2.11 Configuring Oracle Identity Manager Server, Design Console, and Remote Manager

If you are configuring Oracle Identity Manager, you must run the Oracle Identity Manager Configuration Wizard to configure the Oracle Identity Manager Server. For more information, see Section 5.9, "Configuring Oracle Identity Manager Server".

You can also configure Oracle Identity Manager Design Console and Oracle Identity Manager Remote Manager, if required. For more information, see the following sections:

- Section 5.10, "Optional: Configuring Oracle Identity Manager Design Console"
- Section 5.11, "Optional: Configuring Oracle Identity Manager Remote Manager"

3.2.12 Starting the Servers

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

Note: The WebLogic domain will not start unless the Database Security Store has already been configured.

4

Configuring Oracle Identity Navigator

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

- Important Note Before You Begin
- Installation and Configuration Roadmap for Oracle Identity Navigator
- Configuring Oracle Identity Navigator in a New WebLogic Domain
- Starting the Servers
- Verifying Oracle Identity Navigator
- Getting Started with Oracle Identity Navigator After Installation

4.1 Important Note Before You Begin

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

4.2 Installation and Configuration Roadmap for Oracle Identity Navigator

Table 4–1 lists the tasks for installing and configuring Oracle Identity Navigator.

Table 4–1 Installation and Configuration Flow for Oracle Identity Navigator

No.	Task	Description
1	Review installation concepts in the Installation Planning Guide.	Read the *Oracle Fusion Middleware Installation Planning Guide*, which describes the process for various users to install or upgrade to Oracle Fusion Middleware 11*g* (11.1.2) depending on the user's existing environment.
2	Review the system requirements and certification documents to ensure that your environment meets the minimum installation requirements for the components you are installing.	For more information, see Section 2.1, "Reviewing System Requirements and Certification".
3	Obtain the Oracle Fusion Middleware Software.	For more information, see Section 3.2.1, "Obtaining the Oracle Fusion Middleware Software"
4	Review the Database requirements.	For more information, see Section 3.2.2, "Database Requirements".

Table 4–1 (Cont.) Installation and Configuration Flow for Oracle Identity Navigator

No.	Task	Description
5	Run Oracle Fusion Middleware Repository Creation Utility (RCU) to create and load the appropriate schemas for Oracle Identity and Access Management products.	For more information, see Section 3.2.3, "Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU)".
6	Review WebLogic Server and Middleware Home requirements.	For more information, see Section 3.2.4, "WebLogic Server and Middleware Home Requirements".
7	Start the Oracle Identity and Access Management Installer.	For more information, see Section 3.2.6, "Starting the Oracle Identity and Access Management Installer".
8	Install the Oracle Identity and Access Management 11*g* software.	Oracle Identity Navigator is included in the Oracle Identity and Access Management Suite. You can use the Oracle Identity and Access Management 11*g* Installer to install Oracle Identity and Access Management Suite. For more information, see Section 3.2.7, "Installing Oracle Identity and Access Management 11g Release 2 (11.1.2.2.0)".
9	Run the Oracle Fusion Middleware Configuration Wizard to configure your Oracle Identity and Access Management products in a new or existing WebLogic domain.	For more information, see Section 4.3, "Configuring Oracle Identity Navigator in a New WebLogic Domain".
10	Configure the Database Security Store.	For more information, see Section 3.2.10, "Configuring Database Security Store for an Oracle Identity and Access Management Domain".
11	Start the servers.	You must start the WebLogic Administration Server. For more information, see Section 4.4, "Starting the Servers".
12	Complete the post-installation tasks.	Complete the following post-installation tasks: ■ Section 4.5, "Verifying Oracle Identity Navigator" ■ Section 4.6, "Getting Started with Oracle Identity Navigator After Installation"

4.3 Configuring Oracle Identity Navigator in a New WebLogic Domain

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

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure

4.3.1 Appropriate Deployment Environment

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

4.3.2 Components Deployed

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

4.3.3 Dependencies

The configuration in this section depends on the following:

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

4.3.4 Procedure

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

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

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

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

2. On the Welcome screen, select **Create a new WebLogic domain**, and click **Next**. The Select Domain Source screen appears.
3. On the Select Domain Source screen ensure that the **Generate a domain configured automatically to support the following products:** option is selected. Select **Oracle Identity Navigator for Managed Server - 11.1.2.2.0 [IAM_Home]**, and click **Next**. The Specify Domain Name and Location screen appears.

   > **Note:** When you select the **Oracle Identity Navigator for Managed Server- 11.1.2.2.0 [IAM_Home]** option, the following options are also selected, by default:
   >
   > - **Oracle Platform Security Service 11.1.1.0 [IAM_Home]**
   > - **Oracle JRF 11.1.1.0 [oracle_common]**

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

6. The Configure Server Start Mode and JDK screen appears. Choose a JDK from the **Available JDKs** and select a **WebLogic Domain Startup Mode**. Click **Next**.
7. On the Configure JDBC Component Schema screen, select a component schema, such as the **OPSS Schema** that you want to modify.

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

   Select the desired options, and click **Next**.

   Note: The default managed server name where Oracle Identity Navigator is deployed is `opam_server1`.
9. Optional: Configure the following Administration Server parameters:
   - Name
   - Listen address
   - Listen port
   - SSL listen port
   - SSL enabled or disabled
10. Optional: Assign the Administration Server to a machine.
11. Optional: Select Deployments, such as applications and libraries, and Services to target them to a particular cluster or server.
12. Optional: Configure RDBMS Security Store, as required.
13. 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.

Note: After configuring Oracle Identity Navigator in a new WebLogic administration domain, you must configure the Database Security Store. For more information, see Section 3.2.10, "Configuring Database Security Store for an Oracle Identity and Access Management Domain".

4.4 Starting the Servers

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

4.5 Verifying Oracle Identity Navigator

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

1. Log in to the Administration Console for Oracle Identity Navigator using the following URL:

   `http://<managedserver-host>:<managedserver-nonsslport>/oinav/faces/idmNag.jspx`

   The Oracle Identity Navigator dashboard and the resource catalog are displayed.

2. Click the **Customize link** on the upper right corner of the screen to switch to the Edit mode.

3. Click the **Add Content** button on the page. A resource catalog pops up.

4. In the pop-up dialog, click the **Open** link for the folder IDM Product Launcher. The Launcher task flow pops up.

5. In the pop-up dialog, click the **Add** link. Verify that the Launcher portlet is added to the page content. Continue to add News task flows to the page, without closing the pop-up dialog. Click the up arrow at the upper left corner. The top folder layout is displayed again. Click the **Open** link for the folder News. The News and Announcements task flow pops up.

6. In the News and Announcements pop-up dialog, click the **Add** link. Verify that the Report portlet is added to the page content. Continue to add Reports task flows to the page, without closing the pop-up dialog. Click the up arrow at the upper left corner. The top folder layout is displayed again. Click the **Open** link for the folder My Reports. Click the **Add** link and the Close button (X). All the three workflows are added to the page content.

7. Change the default layout, if necessary, by clicking the Pencil icon located on the upper right area of the screen.

8. To exit the Edit mode, click the **Close** button.

   If the task flows are properly added to the page content, the screen displays the task flow content.

9. Test the Product Registration functionality as follows:

   a. Create, edit, or delete the product information by clicking the **Administration** tab.

   b. To add a new product, click the **Create image** icon in the Product Registration section. The New Product Registration dialog pops up.

   c. Enter the relevant information in this dialog, and the new product registration is updated accordingly. The new product registration data is updated on the Launcher portlet after you click the **Dashboard** tab.

   d. Click the product link and ensure that a new browser window or tab opens with the registered product URL.

10. Test the News functionality as follows:

a. Click the **refresh** icon to update the RSS feed content.

b. Click the news item link to open the source of content in a new browser window or tab.

11. Test the Reports functionality as follows:

a. Add a report by clicking the **Add** icon. The Add Report dialog pops up.

b. In this dialog, select a report to add, and click the **Add Report** button. Verify that the report is added.

c. Run a report by clicking the report icon. The report opens in a new browser window or tab.

4.6 Getting Started with Oracle Identity Navigator After Installation

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

5

Configuring Oracle Identity Manager

This chapter explains how to configure Oracle Identity Manager.

It includes the following topics:

- Important Notes Before You Start Configuring Oracle Identity Manager
- Installation and Configuration Roadmap for Oracle Identity Manager
- Creating a new WebLogic Domain for Oracle Identity Manager and SOA
- Upgrading Oracle Platform Security Services Schema
- Configuring Database Security Store
- Starting the Servers
- Overview of Oracle Identity Manager Configuration
- Starting the Oracle Identity Manager 11g Configuration Wizard
- Configuring Oracle Identity Manager Server
- Optional: Configuring Oracle Identity Manager Design Console
- Optional: Configuring Oracle Identity Manager Remote Manager
- Verifying the Oracle Identity Manager Installation
- Changing Memory Settings for Oracle Identity Manager
- Setting Up Integration with Oracle Access Management
- List of Supported Languages
- Using the Diagnostic Dashboard
- Getting Started with Oracle Identity Manager After Installation

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

5.1 Important Notes Before You Start Configuring Oracle Identity Manager

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

- **IAM_HOME** is used to refer to the Oracle Home directory that includes Oracle Identity Manager, Oracle Access Management, Oracle Adaptive Access Manager,

Oracle Entitlements Server, Oracle Identity Navigator, Oracle Privileged Account Manager, and Oracle Access Management Mobile and Social. You can specify any name for this Oracle Home directory.

- By performing the domain configuration procedures described in this chapter, you can create Managed Servers on a local machine (the machine on which the Administration Server is running). However, you can create and start Managed Servers for Oracle Identity and Access Management components on a remote machine. For more information, see the "Creating and Starting a Managed Server on a Remote Machine" topic in the *Oracle Fusion Middleware Creating Templates and Domains Using the Pack and Unpack Commands* guide.
- You must use the Oracle Identity Manager Configuration Wizard to configure Oracle Identity Manager Server, Oracle Identity Manager Design Console (on Windows only), and Oracle Identity Manager Remote Manager.

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

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

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

5.2 Installation and Configuration Roadmap for Oracle Identity Manager

Table 5–1 lists the tasks for installing and configuring Oracle Identity Manager.

Table 5–1 Installation and Configuration Flow for Oracle Identity Manager

No.	Task	Description
1	Review installation concepts in the Installation Planning Guide.	Read the *Oracle Fusion Middleware Installation Planning Guide*, which describes the process for various users to install or upgrade to Oracle Fusion Middleware 11*g* (11.1.2) depending on the user's existing environment.
2	Review the system requirements and certification documents to ensure that your environment meets the minimum installation requirements for the components you are installing.	For more information, see Section 2.1, "Reviewing System Requirements and Certification".
3	Obtain the Oracle Fusion Middleware Software.	For more information, see Section 3.2.1, "Obtaining the Oracle Fusion Middleware Software"

Table 5–1 (Cont.) Installation and Configuration Flow for Oracle Identity Manager

No.	Task	Description
4	Review the Database requirements.	For more information, see Section 3.2.2, "Database Requirements".
5	Run Oracle Fusion Middleware Repository Creation Utility (RCU) to create and load the appropriate schemas for Oracle Identity and Access Management products.	For more information, see Section 3.2.3, "Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU)".
6	Review WebLogic Server and Middleware Home requirements.	For more information, see Section 3.2.4, "WebLogic Server and Middleware Home Requirements".
7	Install Oracle SOA Suite 11*g* (11.1.1.7.0).	Install the 11.1.1.7.0 version of Oracle SOA Suite. For more information, see Section 3.2.5, "Installing Oracle SOA Suite (Oracle Identity Manager Users Only)". **Note:** After installing Oracle SOA Suite 11.1.1.7.0, you must apply mandatory SOA patches before installing Oracle Identity Manager. For more information, see "SOA Patch Requirements for Oracle Identity Manager".
8	Start the Oracle Identity and Access Management Installer.	For more information, see Section 3.2.6, "Starting the Oracle Identity and Access Management Installer".
9	Install the Oracle Identity and Access Management 11*g* software.	Oracle Identity Manager is included in the Oracle Identity and Access Management Suite. You can use the Oracle Identity and Access Management 11*g* Installer to install Oracle Identity and Access Management Suite. For more information, see Section 3.2.7, "Installing Oracle Identity and Access Management 11g Release 2 (11.1.2.2.0)".
10	Run the Oracle Fusion Middleware Configuration Wizard to configure your Oracle Identity and Access Management products in a new or existing WebLogic domain.	For more information, see Section 5.3, "Creating a new WebLogic Domain for Oracle Identity Manager and SOA"
11	Upgrade the OPSS schema using Patch Set Assistant.	For more information, see Section 5.4, "Upgrading Oracle Platform Security Services Schema"
12	Configure the Database Security Store.	For more information, see Section 5.5, "Configuring Database Security Store".
13	Start the servers.	You must start the Administration Server and the SOA Managed Server. For more information, see Section 5.6, "Starting the Servers".
14	Review the Oracle Identity Manager Server, Design Console, and Remote Manager configuration scenarios.	For more information, see Section 5.7, "Overview of Oracle Identity Manager Configuration".
15	Start the Oracle Identity Manager 11g Configuration Wizard.	For more information, see Section 5.8, "Starting the Oracle Identity Manager 11g Configuration Wizard".
16	Configure Oracle Identity Manager Server.	For more information, see Section 5.9, "Configuring Oracle Identity Manager Server".

Table 5–1 (Cont.) Installation and Configuration Flow for Oracle Identity Manager

No.	Task	Description
17	Optional: Install and Configure only Oracle Identity Manager Design Console on Windows.	For more information, see Section 5.10, "Optional: Configuring Oracle Identity Manager Design Console".
18	Optional: Configure Oracle Identity Manager Remote Manager.	For more information, see Section 5.11, "Optional: Configuring Oracle Identity Manager Remote Manager".
19	Complete the post-installation tasks.	Complete the following post-installation tasks: ■ Section 5.12, "Verifying the Oracle Identity Manager Installation" ■ Section 5.14, "Setting Up Integration with Oracle Access Management" ■ Section 5.15, "List of Supported Languages" ■ Section 5.16, "Using the Diagnostic Dashboard" ■ Section 5.17, "Getting Started with Oracle Identity Manager After Installation"

5.3 Creating a new WebLogic Domain for Oracle Identity Manager and SOA

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

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure

5.3.1 Appropriate Deployment Environment

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

5.3.2 Components Deployed

Performing the configuration in this section installs the following components:

- Administration Server
- Managed Servers for Oracle Identity Manager and SOA.
- Oracle Identity Manager System Administration Console, and Oracle Identity Manager Self Service Console on the Oracle Identity Manager Managed Server

5.3.3 Dependencies

The configuration in this section depends on the following:

- Oracle WebLogic Server 11*g* Release 1 (10.3.6)
- Installation of the Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0) software

- Installation of Oracle SOA Suite 11*g* (11.1.1.7.0)
- Database schemas for Oracle Identity Manager and Oracle SOA 11*g* Suite

5.3.4 Procedure

Complete the following steps to create a new WebLogic domain for Oracle Identity Manager and SOA:

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

   Select **Oracle Identity Manager - 11.1.2.0.0 [IAM_Home]**. When you select the **Oracle Identity Manager - 11.1.2.0.0 [IAM_Home]** option, the following options are also selected, by default:

   - **Oracle SOA Suite - 11.1.1.1.0 [Oracle_SOA1]**
   - **Oracle Enterprise Manager 11.1.1.0 [oracle_common]**
   - **Oracle Platform Security Service 11.1.1.0 [IAM_Home]**
   - **Oracle JRF 11.1.1.0 [oracle_common]**
   - **Oracle JRF WebServices Asynchronous services - 11.1.1.0 [oracle_common]**
   - **Oracle WSM Policy Manager 11.1.1.0 [oracle_common]**

Note:

- If you want to use Authorization Policy Manager for the new WebLogic domain for Oracle Identity Manager, then you must select the **Oracle Entitlements Server for Admin Server- 11.1.1.0 [IAM_Home]** option.
- If you have an existing WebLogic domain for Oracle Identity Manager, and you want to use Authorization Policy Manager, then you must perform the following steps:

    1. On the Welcome screen of the Oracle Fusion Middleware Configuration Wizard, select **Extend an existing WebLogic domain**, and click **Next**.
    2. On the Select a WebLogic Domain Directory screen, select the directory that contains the domain in which you configured Oracle Identity Manager. Click **Next**.
    3. On the Select Extension Source screen, ensure that the **Extend my domain to automatically to support the following added products:** is selected, and select **Oracle Entitlements Server for Admin Server- 11.1.1.0 [IAM_Home]** or **Oracle Entitlements Server for Managed Server- 11.1.1.0 [IAM_Home]** option. Click **Next**.
    4. The Configure JDBC Component Schema screen appears. Continue with step 9. Note that for step 9, Administration Server and RDBMS Security Store options are not available when you are extending a domain.

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

5. Enter a name and a location for the domain to be created, and click **Next**. The Configure Administrator User Name and Password screen appears.
6. Configure a user name and a password for the administrator. The default user name is `weblogic`. Click **Next**.
7. The Configure Server Start Mode and JDK screen appears. Choose a JDK from the **Available JDKs** and select a **WebLogic Domain Startup Mode**. Click **Next**.
8. 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

- OPSS Schema

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 the **Administration Server**, **JMS Distributed Destination**, **Managed Servers, Clusters, and Machines**, **Deployments and Services**, **JMS File Store**, and **RDBMS Security Store**. Click **Next**.
11. Optional: Configure the following Administration Server parameters:
    - Name
    - Listen address
    - Listen port
    - SSL listen port
    - SSL enabled or disabled

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

    Note: On the Configure Managed Servers screen, if the **Listen address** for SOA Managed Server is not specified, then it is assumed that SOA server is running on a localhost.

    If you are planning to configure SOA Managed Server on a different host, then you must specify the **Listen address** for the SOA Managed Server, when you are creating a new WebLogic domain for Oracle Identity Manager and SOA.

14. Optional: Configure Clusters, as required. Click **Next**.

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

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

17. Optional: Assign servers to machines. Click **Next**.
18. Optional: Select Deployments, such as applications and libraries, and Services to target them to a particular cluster or server. Click **Next**.

19. 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.

5.4 Upgrading Oracle Platform Security Services Schema

After you create a WebLogic domain for Oracle Identity Manager and SOA, you must upgrade the Oracle Platform Security Services schema using the Patch Set Assistant. For more information, see Section 3.2.9, "Upgrading OPSS Schema using Patch Set Assistant".

5.5 Configuring Database Security Store

After you upgrade the OPSS schema, you must configure the database security store by running the `configureSecurityStore.py` script. For more information, see Section 3.2.10, "Configuring Database Security Store for an Oracle Identity and Access Management Domain".

5.6 Starting the Servers

After installing and configuring Oracle Identity Manager in a WebLogic domain, you must start the Oracle WebLogic Administration Server and the SOA Managed Server. For more information, see Appendix C.1, "Starting the Stack".

Notes:

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

5.7 Overview of Oracle Identity Manager Configuration

This section discusses the following topics:

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

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

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

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

This section discusses the following topics:

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

5.7.1.1 Prerequisites for Configuring Oracle Identity Manager Server

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

1. Installing a supported version of Oracle database. For more information, see Section 3.2.2, "Database Requirements".
2. Creating and loading the required schemas in the database. For more information, see Section 3.2.3, "Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU)".
3. Installing Oracle WebLogic Server and creating a Middleware Home directory. For more information, see Section 3.2.4, "WebLogic Server and Middleware Home Requirements".
4. Installing Oracle SOA Suite 11*g* Release 1(11.1.1.7.0) under the same Middleware Home directory. For more information, see Section 3.2.5, "Installing Oracle SOA Suite (Oracle Identity Manager Users Only)".
5. Installing the Oracle Identity and Access Management Suite (the suite that contains Oracle Identity Manager, Oracle Access Management, Oracle Adaptive Access Manager, Oracle Entitlements Server, Oracle Privileged Account Manager, Oracle Identity Navigator, and Oracle Access Management Mobile and Social) under the Middleware Home directory. For more information, see Section 3.2.7, "Installing Oracle Identity and Access Management 11g Release 2 (11.1.2.2.0)".
6. Creating a new WebLogic domain or extending an existing Identity Management 11.1.1.6.0 domain for Oracle Identity Manager and Oracle SOA. For more information, see Section 5.3, "Creating a new WebLogic Domain for Oracle Identity Manager and SOA".
7. Starting the Oracle WebLogic Administration Server for the domain in which the Oracle Identity Manager application is deployed. For more information, see Appendix C.1, "Starting the Stack".
8. Starting the SOA Managed Server, as described in Appendix C.1, "Starting the Stack".

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

On the machine where you are installing and configuring Design Console, you must install the Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0) software containing Oracle Identity Manager, Oracle Access Management, Oracle Adaptive Access Manager, Oracle Entitlements Server, Oracle Identity Navigator, Oracle Privileged Account Manager, and Oracle Access Management Mobile and Social. For information, see Section 3.2.7, "Installing Oracle Identity and Access Management 11g Release 2 (11.1.2.2.0)".

Before you can configure Oracle Identity Manager Design Console by running the Oracle Identity Manager Configuration Wizard, you should have configured the Oracle Identity Manager Server, as described in Section 5.9, "Configuring Oracle Identity Manager Server" on a local or remote machine. In addition, the Oracle Identity Manager Server should be up and running.

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

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

On the machine where you are installing and configuring Remote Manager, you must install the Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0) software containing Oracle Identity Manager, Oracle Access Management, Oracle Adaptive Access Manager, Oracle Entitlements Server, Oracle Identity Navigator, Oracle Privileged Account Manager, and Oracle Access Management Mobile and Social. For information, see Section 3.2.7, "Installing Oracle Identity and Access Management 11g Release 2 (11.1.2.2.0)".

Before you can configure Oracle Identity Manager Remote Manager by running the Oracle Identity Manager Configuration Wizard, you should have configured the Oracle Identity Manager Server, as described in Section 5.9, "Configuring Oracle Identity Manager Server". In addition, the Oracle Identity Manager Server should be up and running.

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

5.7.2 Oracle Identity Manager Configuration Scenarios

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

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

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

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

This section discusses the following topics:

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

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

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

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

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

Perform the following tasks:

1. Install and configure Oracle Identity Manager Server on a machine after completing all of the prerequisites, as described in Section 5.9, "Configuring Oracle Identity Manager Server". Ensure that the Oracle Identity Manager Server is up and running.
2. On the Windows machine on which the Design Console is to be installed, install a JDK in a path without a space such as `c:/jdk1.6.0_29`.
3. Install Oracle WebLogic Server and create a Middleware Home directory such as `c:/oracle/Middleware`.
4. Run `setup.exe` from the installation media `disk1` and follow the prompts selecting the `Middleware_Home` created above.

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

5. The installer will install the Oracle Identity and Access Management suite needed to install the Design Console.
6. On the Windows machine where you installed the Oracle Identity and Access Management 11*g* software, run the Oracle Identity Manager Configuration Wizard to configure only Design Console. Note that you must provide the Oracle Identity Manager Server information, such as host and URL, when configuring Design Console. For more information, see Section 5.10, "Optional: Configuring Oracle Identity Manager Design Console".

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

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

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

1. Install and configure Oracle Identity Manager Server on a machine after completing all of the prerequisites, as described in Section 5.9, "Configuring Oracle Identity Manager Server". Ensure that the Oracle Identity Manager Server is up and running.

> **Note:** Ensure that you install the same JDK vendor and JDK version, as the one used for the Oracle Identity Manger Server installation, in the client machine where you are installing the Remote Manager.

2. On a different machine, install the Oracle Identity and Access Management 11*g* software containing Oracle Identity Manager, Oracle Access Management, Oracle Adaptive Access Manager, Oracle Entitlements Server, Oracle Identity Navigator, Oracle Privileged Account Manager, and Oracle Access Management Mobile and Social. For information, see Section 3.2.7, "Installing Oracle Identity and Access Management 11g Release 2 (11.1.2.2.0)".
3. On the machine where you installed the Oracle Identity and Access Management 11*g* software, run the Oracle Identity Manager Configuration Wizard to configure only Remote Manager. Note that you must provide the Oracle Identity Manager Server information, such as host and URL, when configuring Remote Manager. For more information, see Section 5.11, "Optional: Configuring Oracle Identity Manager Remote Manager".

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

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

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

1. Install and configure Oracle Identity Manager Server on a machine after completing all the prerequisites, as described in Section 5.9, "Configuring Oracle Identity Manager Server". Ensure that the Oracle Identity Manager Server is up and running.
2. On the same machine, configure Design Console, as described in Section 5.10, "Optional: Configuring Oracle Identity Manager Design Console".
3. On the same machine, configure Remote Manager, as described in Section 5.11, "Optional: Configuring Oracle Identity Manager Remote Manager".

5.8 Starting the Oracle Identity Manager 11*g* Configuration Wizard

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

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

5.9 Configuring Oracle Identity Manager Server

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

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

5.9.1 Appropriate Deployment Environment

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

5.9.2 Components Deployed

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

5.9.3 Dependencies

The installation and configuration in this section depends on Oracle WebLogic Server, on Oracle SOA Suite, and on the installation of Oracle Identity and Access Management 11*g* software. For more information, see Chapter 2, "Preparing to Install" and Section 3.2.7, "Installing Oracle Identity and Access Management 11g Release 2 (11.1.2.2.0)".

5.9.4 Procedure

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

1. Ensure that all the prerequisites, described in Section 5.7.1.1, "Prerequisites for Configuring Oracle Identity Manager Server", are satisfied. In addition, see Section 5.1, "Important Notes Before You Start Configuring Oracle Identity Manager".
2. On the machine where the Administration Server is running, start the Oracle Identity Manager Configuration Wizard, as described in Section 5.8, "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:instancename1^hostname2:port2:instancename2@servicename
   ```

   Note: You can use the same database or different databases for creating the Oracle Identity Manager schema and the Metadata Services schema.

   Ensure that no Firewalls/Gateways are preventing the connection to the database.
5. In the **OIM Schema User Name** field, enter the name of the schema that you created for Oracle Identity Manager using the Oracle Fusion Middleware Repository Creation Utility (RCU). For more information, see Section 3.2.3, "Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU)".
6. In the **OIM Schema Password** field, enter the password for the Oracle Identity Manager schema that you set while creating the schema using the Oracle Fusion Middleware Repository Creation Utility (RCU).
7. If you want to use a different database for the Metadata Services (MDS) schema, select the **Select different database for MDS Schema** check box.

8. If you choose to use a different database for MDS schema, in the **MDS Connect String** field, enter the full path, listen port, and service name for the database associated with the MDS schema. For the format of the connect string, see Step 4.

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

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

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

   `t3://hostname:port`

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

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

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

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

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

12. **OIM HTTP URL**

    - The OIM HTTP URL is of the format: `http(s)://<host>:<port>`. For example, `https://localhost:7002`.
    - For single node deployments where OIM managed server is not front-ended with Oracle HTTP Server, you can provide OIM managed server's URL.
    - For single node deployments where OIM managed server is frontended with Oracle HTTP Server, you must provide the http URL that front-ends the Oracle Identity Manager application.
    - For cluster deployments, provide the load balancer URL that frontends the OIM cluster.

13. **OIM External Front End URL**

    - The OIM External Front End URL is of the format: `http(s)://<host>:<port>`. For example, `https://localhost:7070`
    - For single node deployments where OIM managed server is not front-ended with Oracle HTTP Server, this field can be left blank.

- For deployments where there is no SSO configured but OIM managed server is front-ended with Oracle HTTP Server, you must provide the http URL that front-ends the Oracle Identity Manager application.
- For deployments where SSO is configured, provide the SSO URL where OIM UI is available.

14. 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.
15. In the **Confirm Keystore Password** field, enter the new password again.
16. Optional: To enable LDAP Sync, you must select the **Enable LDAP Sync** option on the OIM Server screen.

    Notes:

    - If you are not planning to integrate Oracle Identity Manager with Oracle Access Management, then do not select the **Enable LDAP Sync** option.
    - If you want to enable LDAP Sync, before enabling LDAP Sync you must complete the steps, as described in Completing the Prerequisites for Enabling LDAP Synchronization.
    - Once LDAP Sync is enabled on the OIM Server screen and prerequisites are completed, you must continue to configure the Oracle Identity Manager Server. After you have configured the Oracle Identity Manager Server and exited the Oracle Identity Management Configuration Wizard, you must run the LDAP post-configuration utility as described in Running the LDAP Post-Configuration Utility.

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

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

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

Notes:

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

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

  For example: `oid1` for OID, `oud1` for OUD, `iplanet1` for IPLANET, and `ad1` for ACTIVE_DIRECTORY
- **Server URL** - enter the LDAP URL in the format `ldap://oid_host:oid_port`.
- **Server User** - enter the user name for Directory Server administrator.

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

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

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

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

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

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

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

    > **Note:** Before configuring an application, you can save your configuration settings and preferences in a response file. Response files are text files that you can create or edit in a text editor. You can use response files to perform a silent installation or use as templates or customized settings for your environment.
    >
    > For information on performing silent installation, refer to the "Silent Oracle Fusion Middleware Installation and Deinstallation" topic in the *Oracle Fusion Middleware Installation Planning Guide for Oracle Identity and Access Management*.

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

    A configuration log is saved to the `logs` directory under Oracle Inventory directory. For information about the log files, see 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.

20. Click **Finish**.

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

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

5.9.5 Completing the Prerequisites for Enabling LDAP Synchronization

You must complete the following prerequisites:

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

5.9.5.1 Preconfiguring the Identity Store

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

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

- OID
- Active Directory
- iPlanet/ODSEE
- OUD
- OVD

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

1. Create User, Group and Reserve Containers.
2. Create the proxy user for OIM, namely `oimadminuser` in the Directory Server outside the search base used for OIM reconciliation. This OIM proxy user should not be reconciled into OIM Database.
3. Create the `oimadmingroup` and assign the `oimadminuser` to the group.
4. Add the ACIs to the group and user container for the OIM proxy user to have access to all entries in those containers.

Note: The preconfiguration differs, depending on the directory store you wish to use to hold your identity information. For a sample procedure of preconfiguring the Identity Store, refer to the following:

- Preconfiguring Oracle Directory Server Enterprise Edition (ODSEE)
- Preconfiguring Oracle Unified Directory (OUD)
- Preconfiguring Oracle Internet Directory (OID)

5. Extend OIM Schema for non-OID Directory Servers.
   - For Active Directory
     - The OIM Schema for Active Directory is in the following location:

       `$MW_HOME/oracle_common/modules/oracle.ovd_11.1.1/oim-templates`

     - Ensure that the environment variable `ORACLE_HOME` is set to the directory where Oracle Identity Manager is deployed.

       For example:

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

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

     - Run the following command to extend Active Directory schema:

       On Windows:

       ```
       extendadschema.bat -h AD_host -p AD_port -D <administrator@mydomain.com> -AD <dc=mydomain,dc=com> -w <AD_password> -OAM <true/false>
       ```

Specify the value of -OAM patameter as true if you want to enable OAM-OIM integration.

Specify the value of -OAM patameter as false if you do not want to enable OAM-OIM integration.

On UNIX:

```
extendadschema.sh -h AD_host -p AD_port -D <administrator@mydomain.com> -q -AD <dc=mydomain,dc=com> -OAM <true/false>
```

Specify the value of -OAM patameter as true if you want to enable OAM-OIM integration.

Specify the value of -OAM patameter as false if you do not want to enable OAM-OIM integration.

Note: The extendadschema script is certified only on Active Directory 2003, 2008 and 2008R2.

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

    ```
    $MW_HOME/oracle_common/modules/oracle.ovd_11.1.1/oim-templates/sunOneSchema.ldif
    ```

  - Run the following command to extend ODSEE schema:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

    For example:

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

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

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

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

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

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

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

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

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

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

ldapadd -h <ODSEE Server> -p <ODSEE port> -D <ODSEE
Admin ID> -w <ODSEE Admin password> -f iPlanet7_user_
index_add.ldif
```

or

```
ldapadd -h <ODSEE Server> -p <ODSEE port> -D <ODSEE
Admin ID> -w <ODSEE Admin password> -f iPlanet7_user_
index_generic.ldif

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

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

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

- For OUD
  – To extend OAM Schema for OUD, locate the following files:

```
$IAM_HOME/oam/server/oim-intg/ldif/ojd/schema/ojd_user_
schema_add.ldif

$IAM_HOME/oam/server/oim-intg/ldif/ojd/schema/ojd_user_
index_generic.ldif

$IAM_HOME/oam/server/oim-intg/ldif/ojd/schema/ojd_oam_
pwd_schema_add.ldif
```

  – Use ldapmodify from the command line to load the following three LDIF files:

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

ldapmodify -h <OUD Server> -p <OUD port> -D <OUD Admin
ID> -w <OUD Admin password> -f ojd_user_schema_add.ldif

ldapmodify -h <OUD Server> -p <OUD Admin SSL port> -D
<OUD Admin ID> -w <OUD Admin password> -Z -X -a -f ojd_
user_index_generic.ldif

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

After all the indexes in `ojd_user_index_generic.ldif` are imported, the indexes must be rebuild, either online or offline.

To rebuild the index Offline:

1) Stop the OUD server by executing the following command:

```
$MW_HOME/asinst_1/OUD/bin/stop-ds
```

2) Rebuild the index one by one for all index attributes mentioned in the file `ojd_user_index_generic.ldif` by executing the following command:

```
$MW_HOME/asinst_1/OUD/bin/rebuild-index -h <OUD Server>
-p <OUD Admin SSL port> -D <OUD Admin ID> -j <password-
file> -X --baseDN <baseDN> --index <attribute>
```

For example:

```
$MW_HOME/asinst_1/OUD/bin/rebuild-index -h localhost -p
5444 -D "cn=Directory Manager" -j pwd.txt -X --baseDN
dc=mycompany,dc=com --index obgroupadministrator
```

3) Restart the OUD server by executing the following command:

```
$MW_HOME/asinst_1/OUD/bin/start-ds
```

To rebuild the index Online:

If you rebuild the index online, the OUD server need not be stopped and restarted.

Rebuild the index one by one for all index attributes mentioned in the file `ojd_user_index_generic.ldif` by executing the following command:

```
$MW_HOME/asinst_1/OUD/bin/rebuild-index -h <OUD Server>
-p <OUD Admin SSL port> -D <OUD Admin ID> -j <password-
file> -X --baseDN <baseDN> --index <attribute>
```

For example:

```
$MW_HOME/asinst_1/OUD/bin/rebuild-index -h localhost -p
5444 -D "cn=Directory Manager" -j pwd.txt -X --baseDN
dc=mycompany,dc=com --index obgroupadministrator
--index obid --index oblocationdn
```

Note: To find out the OUD Admin SSL port, check the configuration in `<OUD Home Directory>/config/config.ldif`, under the entry `cn=Administration Connector,cn=config`. It is the value associated to the attribute `ds-cfg-listen-port`.

For example:

`$MW_HOME/asinst_1/OUD/config/config.ldif` has `5444` as OUD Admin SSL port.

```
dn: cn=Administration Connector,cn=config

objectClass: ds-cfg-administration-connector

objectClass: top

ds-cfg-listen-address: 0.0.0.0

ds-cfg-listen-port: 5444
```

---

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

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

5.9.5.2 Creating Adapters in Oracle Virtual Directory

Oracle Virtual Directory communicates with other directories through adapters.

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

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

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

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

For example:

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

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

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

5.9.5.2.1 Creating Adapters for Oracle Internet Directory

User Adapter

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

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

Note: The default port number is 7005.

---

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

Table 5–2 Parameters for User Adapter Creation

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

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

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

Table 5–3 User Adapter Parameter Values

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

   e. Click **OK**.

f. Click **Apply**.

Change Log Adapter

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

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

   Note: The default port number is 7005.

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

Table 5–4 Parameters for Change Log Adapter Creation

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

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

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

      Edit the Change Log Adapter to either add or modify the properties so that they match the values shown in the following table. You must add the

modifierDNFilter, sizeLimit, and targetDNFilter properties to the adapter.

Table 5–5 Changelog Adapter Parameter Values

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

e. Click **OK**.

f. Click **Apply**.

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

Restarting Oracle Virtual Directory

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

5.9.5.2.2 Creating Adapters for Microsoft Active Directory Server

User Adapter

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

1. Start the Administration Server and the ODSM Managed Server as described in Appendix C, "Starting or Stopping the Oracle Stack".

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

   Note: The default port number is 7005.

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

Table 5–6 Parameters for New User Adapter Creation

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

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

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

Table 5–7 User Adapter Parameter Values

Parameter	Value
directoryType	`activedirectory`
mapAttribute	`orclguid=objectGuid`

Table 5–7 (Cont.) User Adapter Parameter Values

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

e. Click **OK**.

f. Click **Apply**.

Important Notes on User Management Plugin Configuration

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

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

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

The User Management plugin has the following configuration parameters:

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

Table 5–8 Language Codes for the MLS Enabled Attributes

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

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

Change Log Adapter

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

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

   Note: The default port number is 7005.

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

Table 5–9 Parameters for New Change Log Adapter Creation

Screen	Field	Value/Step
Type	**Adapter Type**	LDAP

Table 5–9 (Cont.) Parameters for New Change Log Adapter Creation

Screen	Field	Value/Step
	Adapter Name	`OIM Change Log Adapter`
	Adapter Template	`Changelog_ActiveDirectory`
Connection	**Use DNS for Auto Discovery**	No
	Host	Active Directory host/virtual name
	Port	389
	Server Proxy Bind DN	`cn=oimAdminUser,cn=systemids,dc=mycompany,dc=com`
	Proxy Password	Password for `oimadmin` user
Connection Test		Validate that the test succeeds
Namespace	**Remote Base**	Remote Base should be empty
	Mapped Namespace	`cn=changelog`

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

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

      Edit the Change Log Adapter to either add or modify the properties so that they match the values shown in Table 5–10. You must add the `sizeLimit`, and `targetDNFilter` properties to the adapter.

Table 5–10 Changelog Adapter Parameter Values

Parameter	Value
directoryType	`activedirectory`
mapAttribute	`targetGUID=objectGuid`
requiredAttribute	samaccountname
sizeLimit	1000
targetDNFilter	Optional parameter. For more information, see Important Notes on Changelog Plugin Configuration.
oamEnabled	`true` or `false` Note that this parameter should be set to `true` only if you are setting up integration between Oracle Identity Manager and Oracle Access Manager at a later time.
mapUserState	`true` For more information, see Important Notes on Changelog Plugin Configuration.

Table 5–10 (Cont.) Changelog Adapter Parameter Values

Parameter	Value
virtualDITAdapterName	The name of the User adapter For more information, see Important Notes on Changelog Plugin Configuration.

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

e. Click **OK**.

f. Click **Apply**.

5.9.5.2.3 Creating Adapters for Oracle Directory Server Enterprise Edition (ODSEE)

User Adapter

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

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

Note: The default port number is 7005.

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

Table 5–11 Parameters for New User Adapter Creation

Screen	Field	Value/Step
Type	**Adapter Type**	`LDAP`
	Adapter Name	`User Adapter`
	Adapter Template	`User_SunOne`
Connection	**Use DNS for Auto Discovery**	No
	Host	Sun Java System Directory Server host/virtual name
	Port	Sun Java System Directory Server port
	Server Proxy Bind DN	`cn=oimAdminUser,cn=systemids,dc=mycompany,dc=com`

Table 5–11 (Cont.) Parameters for New User Adapter Creation

Screen	Field	Value/Step
	Proxy Password	Password for `oimadmin` user (`cn=oimAdminUser,cn=systemids,dc=mycompany,dc=com`)
Connection Test		Validate that the test succeeds.
Namespace	**Remote Base**	`dc=mycompany,dc=com`
	Mapped Namespace	`dc=mycompany,dc=com`

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

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

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

Table 5–12 User Adapter Parameter Values

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

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

Change Log Adapter

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

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

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

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

Table 5–13 Parameters for New Change Log Adapter Creation

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

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

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

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

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

Table 5–14 Changelog Adapter Parameter Values

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

e. Click **OK**.

f. Click **Apply**.

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

5.9.5.2.4 Creating Adapters for Oracle Unified Directory (OUD)

User Adapter

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

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

Note: The default port number is 7005.

---

3. Connect to Oracle Virtual Directory by using the appropriate connection entry.

4. On the Home page, click on the **Adapter** tab.
5. Start the New Adapter Wizard by clicking on **Create Adapter** at the top of the adapter window.
6. Create a new adapter using the New Adapter Wizard, with the following parameters:

Table 5–15 Parameters for New User Adapter Creation

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

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

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

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

Table 5–16 User Adapter Parameter Values

Parameter	Value
directoryType	`oud`
mapObjectclass	`container=orclContainer`
pwdMaxFailure	`10`

Table 5–16 (Cont.) User Adapter Parameter Values

Parameter	Value
oamEnabled	`true` or `false` Note that this parameter should be set to `true` only if you are setting up integration between Oracle Identity Manager and Oracle Access Manager at a later time.

e. Click **OK**.

f. Click **Apply**.

Change Log Adapter

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

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

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

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

Table 5–17 Parameters for New Change Log Adapter Creation

Screen	Field	Value/Step
Type	**Adapter Type**	`LDAP`
	Adapter Name	`OIM Change Log Adapter`
	Adapter Template	`Changelog_OUD`
Connection	**Use DNS for Auto Discovery**	No
	Host	Oracle Unified Directory Server host virtual name
	Port	Oracle Unified Directory Server port
	Server Proxy Bind DN	`cn=oimAdminUser,cn=systemids,dc=mycompany,dc=com`
	Proxy Password	Password for `oimadmin` user. (`cn=oimAdminUser,cn=systemids,dc=mycompany,dc=com`)
Connection Test		Validate that the test succeeds.
Namespace	**Remote Base**	Remote Base should be empty
	Mapped Namespace	`cn=changelog`

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

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

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

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

Table 5–18 Changelog Adapter Parameter Values

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

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

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

5.9.5.2.5 Important Notes on Changelog Plugin Configuration

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

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

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

  If you configure the **virtualDITAdapterName** parameter in changelog plugin with the same value as the name of the User Adapter, it also performs the user management adapter mapping that is required in the changelog adapter.

  The **virtualDITAdapterName** parameter also determines the DN mapping from the backend LDAP store to OVD (for the changelog adapter).

  For example, if customer needs a way to create a map for the **Change Log Adapter**, which has a root of `cn=changelog` to return values as `cn=users,ou=oim,dc=aglc,dc=ca` , when they are actually coming from the LDAP node `cn=users,dc=aglc,dc=ca`, then the solution is to configure **virtualDITAdapterName** in changelog plugin to have the value of the **User adapter**.

  Note: Configuring **virtualDITAdaptername** is a mandatory step for directoryType=ActiveDirectory

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

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

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

  For example:

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

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

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

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

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

5.9.6 Running the LDAP Post-Configuration Utility

You must run the LDAP post-configuration utility after you have configured the Oracle Identity Manager Server and exited the Oracle Identity Manager Configuration Wizard. The LDAP configuration post-setup script enables all the LDAP Sync-related incremental Reconciliation Scheduler jobs, which are disabled by default. In addition, it retrieves the last change number from the Directory Server and updates all the LDAPSync Incremental Reconciliation jobs.

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

Setting Up Environment Variables

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

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

  For example:

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

  On Windows, it is the `<MW_HOME>\IAM_Home` directory.
- *WL_HOME* - is set to the `wlserver_10.3` directory under your Middleware Home.

  For example:

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

  On Windows, it is the `<MW_HOME>\wlserver_10.3` directory.
- *DOMAIN_HOME* - is set to the domain of the WebLogic Server.

  For example:

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

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

Running the LDAP Post-Configuration Utility

Run the LDAP post-configuration utility as follows:

Note: Before running the LDAP post configuration utility, you must create ACLs for the proxy users or the ACL disabled users.

---

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

     For example:

     OIMServerType=WLS
   - **OIMProviderURL** - Specify the URL for the OIM provider.

     If the OIMServerType is WLS, then

     OIMProviderURL=t3://localhost:ManagedServerPort

     For example:

     OIMProviderURL=t3://localhost:14000
   - **LDAPURL** - Specify the URL for the OVD instance.

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

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

     For example:

     LDAPURL=ldap://OVDserver.examplehost.exampledomain.com:6501

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

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

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

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

For example:

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

Notes:

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

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

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

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

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

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

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

  Special Instructions for Windows Users:

  When you specify the value for the **LIBOVD_PATH_PARAM** parameter on Windows, you must note the following:

  1. The value should start with forward slash or "/"

  2. Use forward slash or "/" as PATH separator on Windows instead of the backslash or "\"

  For example:

  On Windows:

  ```
  LIBOVD_PATH_PARAM=/C:/MW_HOME/user_projects/domains/base_
  domain/config/fmwconfig/ovd/oim
  ```

  On UNIX:

  ```
  LIBOVD_PATH_PARAM=/MW_HOME/user_projects/domains/base_
  domain/config/fmwconfig/ovd/oim
  ```

Notes:

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

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

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

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

   On Windows:

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

   For example:

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

   On UNIX:

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

   For example:

   ```
   LDAPConfigPostSetup.sh <MW_Home>/IAM_Home/server/ldap_config_
   util
   ```
6. When prompted, enter the OIM administrator's password and the LDAP administrator password as applicable.

Notes:

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

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

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

5.9.7 Verifying the LDAP Synchronization

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

1. Ensure that the WebLogic Administration Server and the Oracle Identity Manager Managed Server is up and running.
2. Invoke the Oracle Identity Manager Administration Console (`http://<host>:<port>/sysadmin)`, 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. You must verify the values provided during the Oracle Identity Manager configuration when enabling LDAPSync with the parameter values here like Search Base, Reservation Container, URL, bind DN.

   For more information, see "Managing IT Resources" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.
4. Create a normal user using the Oracle Identity Manager Self Service Console:

   `http://<host>:<port>/identity`
5. If a user is created, verify the creation in the chosen LDAP store or OVD using any ldap client.

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

5.9.8 Post-Configuration Steps

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

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

  On Windows:

Open the <IAM_Home>\server\bin\setenv.bat file and search for *XEL_HOME* variable. Update the path of the *XEL_HOME* variable to the absolute path of <IAM_Home>\server.

For example, if your *IAM_Home* is the C:\oracle\Middleware\IAM_Home directory, then set *XEL_HOME* in the setenv.bat file to the C:\oracle\Middleware\IAM_Home\server directory.

On UNIX:

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

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

- If you are extending an Oracle Identity Manager domain to include Oracle Privileged Account Manager, you must complete the following steps:

  1. Go to <DOMAIN_HOME>/config/fmwconfig directory. Create a backup of the jps-config.xml file.
  2. Edit the jps-config.xml file. Locate the section of the file containing jpsContexts, as shown below:

```
<jpsContexts default="default">
        <jpsContext name="default">
            <serviceInstanceRef ref="credstore.db"/>
            <serviceInstanceRef ref="keystore.db"/>
            <serviceInstanceRef ref="policystore.db"/>
            <serviceInstanceRef ref="audit.db"/>
            <serviceInstanceRef ref="idstore.oim"/>
            <serviceInstanceRef ref="trust"/>
            <serviceInstanceRef ref="pdp.service"/>
            <serviceInstanceRef ref="attribute"/>
            <serviceInstanceRef ref="sso.inst.0"/>
        </jpsContext>
```

  3. Make a copy of the above entry and change <jpsContext name="default"> to <jpsContext name="oim">
  4. Edit the original entry and change <serviceInstanceRef ref="idstore.oim"/> to <serviceInstanceRef ref="idstore.ldap"/>
  5. After you have edited the file, the final version of the file should look like the one shown below:

```
<jpsContexts default="default">
        <jpsContext name="default">
            <serviceInstanceRef ref="credstore.db"/>
            <serviceInstanceRef ref="keystore.db"/>
            <serviceInstanceRef ref="policystore.db"/>
            <serviceInstanceRef ref="audit.db"/>
            <serviceInstanceRef ref="idstore.ldap"/>
            <serviceInstanceRef ref="trust"/>
            <serviceInstanceRef ref="pdp.service"/>
            <serviceInstanceRef ref="attribute"/>
            <serviceInstanceRef ref="sso.inst.0"/>
        </jpsContext>
        <jpsContext name="oim">
```

```
        <serviceInstanceRef ref="credstore.db"/>
        <serviceInstanceRef ref="keystore.db"/>
        <serviceInstanceRef ref="policystore.db"/>
        <serviceInstanceRef ref="audit.db"/>
        <serviceInstanceRef ref="idstore.oim"/>
        <serviceInstanceRef ref="trust"/>
        <serviceInstanceRef ref="pdp.service"/>
        <serviceInstanceRef ref="attribute"/>
        <serviceInstanceRef ref="sso.inst.0"/>
    </jpsContext>
```

6. Save the `jps-config.xml` file.
7. Log in to Oracle Enterprise Manager Fusion Middleware Control using your WebLogic Server administrator credentials.

   Note: Before logging in to Oracle Enterprise Manager Fusion Middleware Control, ensure that the Oracle Identity Manager Managed server is up and running.

8. Click on **Identity and Access** > **oim** > **oim(11.1.1.2.0)**. Right-click and select **System MBean Browser**. The System MBean Browser page is displayed.
9. Select Application Defined MBeans.
10. Under Application Defined MBeans, select `oracle.as.soainfra.config > Server:<soa_server> > WorkflowIdentityConfig > human-workflow > WorkflowIdentityConfig.ConfigurationType > jazn.com > WorkflowIdentityConfig.ConfigurationType.ProviderType > JpsProvider > WorkflowIdentityConfig.ConfigurationType.ProviderType.PropertyType`
11. Click on `jpsContextName` and change the **Value** to `oim`.
12. Click **Apply**.
13. Restart the WebLogic Administration Server, SOA Managed Server, and Oracle Identity Manager Managed Server, as described in Appendix C.1, "Starting the Stack"

5.9.9 Setting oamEnabled Parameter for Identity Virtualization Library

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

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

   `http://adminvhn.mycompany.com:7001/em` as user `weblogic`.
2. Go to **Weblogic Domain -> base_domain**. Right click on **Oim(11.1.1.3.0)**, and click **System Mbean Browser**.
3. Go to: **Application defined MBeans** -> **com.oracle** -> **Domain:base_domain** -> **OVD**

4. You will see **AdaptersConfig** options. Click on the one that has a plus (+) symbol, indicating a subtree. Then click on **OVDAdaptersConfig**. You should see **CHANGELOG_oid1** and **oid1**.

   Note that the examples used in this document refers to an adapter named **oid1**, which is the adapter containing UserManagement. There may be other adapters too which are also named **oid1** in other contexts (like default ids which are created OOTB). But the examples used in this guide refers to the adapter **oid1** only in the OIM context.

5. Configure **oamenabled** in both the adapters.

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

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

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

   c. Click on **removeParam operation**.

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

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

   f. Click on **AddParam** operation.

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

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

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

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

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

   c. Click on **removeParam operation**.

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

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

   f. Click on **AddParam** operation.

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

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

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

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

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

5.10 Optional: Configuring Oracle Identity Manager Design Console

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

It includes the following sections:

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

5.10.1 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.

5.10.2 Components Deployed

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

5.10.3 Dependencies

The installation and configuration in this section depends on the installation of Oracle Identity and Access Management 11*g* software and on the configuration of Oracle Identity Manager Server. For more information, see Installing Oracle Identity and Access Management 11g Release 2 (11.1.2.2.0) and Configuring Oracle Identity Manager Server.

5.10.4 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 Oracle Identity Manager Design Console on a Different Machine, are satisfied. In addition, see Important Notes Before You Start Configuring Oracle Identity Manager.
2. On the Windows machine where Oracle Identity Manager Design Console should be configured, start the Oracle Identity Manager Configuration Wizard, as described in 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 Manager 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 information on performing silent installation, refer to the "Silent Oracle Fusion Middleware Installation and Deinstallation" topic in the *Oracle Fusion Middleware Installation Planning Guide for Oracle Identity and Access Management*.

   After you click **Configure**, the Configuration Progress screen appears. A configuration log is saved to the `logs` directory under Oracle Inventory directory. For information about the log files, see 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.

5.10.5 Post-Configuration Steps

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

1. On the machine where Oracle WebLogic Server is installed (the machine where Oracle Identity Manager Server is installed), create the `wlfullclient.jar` file as follows:

   a. Use the `cd` command to move from your present working directory to the `<MW_HOME>\wlserver_10.3\server\lib` directory.

   b. Ensure that *JAVA_HOME* is set, as in the following example:

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

      To set this variable, right-click the **My Computer** icon and select **Properties**. The System Properties screen is displayed. Click the **Advanced** tab and click the **Environment Variables** button. The Environment Variables screen is

displayed. Ensure that the *JAVA_HOME* variable in the **User Variables** section is set to the path of the JDK directory installed on your machine.

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

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

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

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

   `cd` WL_HOME`/server/lib`

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

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

   This command generates the `wlfullclient.jar` file.

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

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

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

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

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

5.10.7 Configuring Design Console to Use SSL

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

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

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

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

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

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

   c. Save the file and exit.

5.11 Optional: Configuring Oracle Identity Manager Remote Manager

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

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure

5.11.1 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.

5.11.2 Components Deployed

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

5.11.3 Dependencies

The installation and configuration in this section depends on the installation of Oracle Identity and Access Management 11*g* software and on the configuration of Oracle Identity Manager Server. For more information, see Installing Oracle Identity and Access Management 11g Release 2 (11.1.2.2.0) and Prerequisites for Configuring Only Oracle Identity Manager Remote Manager on a Different Machine.

5.11.4 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 Oracle Identity Manager Remote Manager on a Different Machine, are satisfied. In addition, see Important Notes Before You Start Configuring Oracle Identity Manager.
2. On the machine where Oracle Identity Manager Remote Manager should be configured, start the Oracle Identity Manager Configuration Wizard, as described in 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 information on performing silent installation, refer to the "Silent Oracle Fusion Middleware Installation and Deinstallation" topic in the *Oracle Fusion Middleware Installation Planning Guide for Oracle Identity and Access Management*.

9. After you click **Configure**, the Configuration Progress screen appears. A configuration log is saved to the `logs` directory under Oracle Inventory directory. For information about the log files, see 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.

5.12 Verifying the Oracle Identity Manager Installation

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

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

You can verify your Oracle Identity Manager installation by:

- Checking the Oracle Identity Manager System Administration URL, such as `http://<Hostname>:<Port>/sysadmin`
- Checking the Oracle Identity Manager Self Service URL, such as `http://<Hostname>:<Port>/identity`
- Verifying the configuration between Oracle Identity Manager and Oracle SOA (BPEL Process Manager) as follows:
  a. Log in to the SOA Infrastructure with WebLogic credentials to verify whether the composite applications are displayed.

     `http://<host>:<bpel_port>/soa-infra`

  b. Log in to the Oracle Identity Manager Self Service Console as an end user:

     `http://<host>:<oim_port>/identity`

  c. Navigate to **My Information**. Modify any attribute and click **Save**. This should raise a request. Logout from self service console.

  d. Log in to the Oracle Identity Manager Self Service Console as `xelsysadm`.

  e. Navigate to **Inbox > Pending Approvals**. 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. Navigate to **Track Requests** and verify whether the request is completed.

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

5.13 Changing Memory Settings for Oracle Identity Manager

For staging and test deployments of Oracle Identity Manager, the maximum heap size of 2 GB is recommended. For the maximum heap size in production deployments, refer to *Oracle Fusion Middleware Performance and Tuning Guide*.

To change the heap setting for Oracle Identity Manager on WebLogic Server:

1. Open the *`DOMAIN_HOME`*`/bin/setOIMDomainEnv.sh` file (on UNIX), or the *`DOMAIN_HOME`*`\bin\setOIMDomainEnv.cmd` file (on Windows).
2. Change `PORT_MEM_ARGS -Xmx` value to `2048m`
3. Save the file.

4. Restart the OIM server. For more information, see Appendix C.3, "Restarting Servers".

5.14 Setting Up Integration with Oracle Access Management

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

5.15 List of Supported Languages

Oracle Identity Manager supports the following languages:

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

5.16 Using the Diagnostic Dashboard

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

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

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

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

5.17 Getting Started with Oracle Identity Manager After Installation

After installing Oracle Identity Manager, refer to "Oracle Identity System Administration Interface" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.

6

Configuring Oracle Access Management

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

- Overview
- Important Note Before You Begin
- Installation and Configuration Roadmap for Oracle Access Management
- Optional: Enabling TDE in Database
- Oracle Access Management in a New WebLogic Domain
- Starting the Servers
- Optional Post-Installation Tasks
- Verifying the Oracle Access Management Installation
- Setting Up Oracle Access Manager Agents
- Setting Up Integration with OIM
- Getting Started with Oracle Access Management After Installation

6.1 Overview

Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0) contains Oracle Access Management which includes the following services:

- Oracle Access Manager
- Oracle Access Management Security Token Service
- Oracle Access Management Identity Federation
- Oracle Access Management Mobile and Social

> **Note:** For an introduction to the Oracle Access Management, see "Oracle Product Introduction" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.

6.2 Important Note Before You Begin

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

Oracle Identity Navigator, Oracle Privileged Account Manager, and Oracle Access Management Mobile and Social. You can specify any name for this Oracle Home directory.

6.3 Installation and Configuration Roadmap for Oracle Access Management

Table 6–1 lists the tasks for installing and configuring Oracle Access Management.

Table 6–1 Installation and Configuration Flow for Oracle Access Management

No.	Task	Description
1	Review installation concepts in the Installation Planning Guide.	Read the *Oracle Fusion Middleware Installation Planning Guide*, which describes the process for various users to install or upgrade to Oracle Fusion Middleware 11*g* (11.1.2) depending on the user's existing environment.
2	Review the system requirements and certification documents to ensure that your environment meets the minimum installation requirements for the components you are installing.	For more information, see Section 2.1, "Reviewing System Requirements and Certification".
3	Obtain the Oracle Fusion Middleware Software.	For more information, see Section 3.2.1, "Obtaining the Oracle Fusion Middleware Software"
4	Review the Database requirements.	For more information, see Section 3.2.2, "Database Requirements". Also see Section 6.4, "Optional: Enabling TDE in Database".
5	Run Oracle Fusion Middleware Repository Creation Utility (RCU) to create and load the appropriate schemas for Oracle Identity and Access Management products.	For more information, see Section 3.2.3, "Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU)".
6	Review WebLogic Server and Middleware Home requirements.	For more information, see Section 3.2.4, "WebLogic Server and Middleware Home Requirements".
7	Start the Oracle Identity and Access Management Installer.	For more information, see Section 3.2.6, "Starting the Oracle Identity and Access Management Installer".
8	Install the Oracle Identity and Access Management 11*g* software.	Oracle Access Management is included in the Oracle Identity and Access Management Suite. You can use the Oracle Identity and Access Management 11*g* Installer to install Oracle Identity and Access Management Suite. For more information, see Section 3.2.7, "Installing Oracle Identity and Access Management 11g Release 2 (11.1.2.2.0)".
9	Run the Oracle Fusion Middleware Configuration Wizard to configure your Oracle Identity and Access Management products in a new or existing WebLogic domain.	For more information, see Section 6.5, "Oracle Access Management in a New WebLogic Domain".
10	Upgrade the OPSS schema using Patch Set Assistant	For more information, see Section 3.2.9, "Upgrading OPSS Schema using Patch Set Assistant"

Table 6–1 (Cont.) Installation and Configuration Flow for Oracle Access Management

No.	Task	Description
11	Configure the Database Security Store.	For more information, see Section 3.2.10, "Configuring Database Security Store for an Oracle Identity and Access Management Domain".
12	Start the servers.	You must start the Administration Server and all Managed Servers. For more information, see Section 6.6, "Starting the Servers".
13	Complete the post-installation tasks.	Complete the following post-installation tasks: ■ Section 6.7, "Optional Post-Installation Tasks" ■ Section 6.8, "Verifying the Oracle Access Management Installation" ■ Section 6.9, "Setting Up Oracle Access Manager Agents" ■ Section 6.10, "Setting Up Integration with OIM" ■ Section 6.11, "Getting Started with Oracle Access Management After Installation"

6.4 Optional: Enabling TDE in Database

Complete the following steps to set up Transparent Data Encryption (TDE) in the database for Oracle Access Management:

1. Add the `ENCRYPTION_WALLET_LOCATION` parameter in the `sqlnet.ora` file of the database.

   ```
   ENCRYPTION_WALLET_LOCATION=(SOURCE=(METHOD=FILE)(METHOD_DATA=
   (DIRECTORY=<DB_WALLET_DIRECTORY>)))
   ```

2. Restart the database.
3. Run the following sql queries as `SYSDBA` to create the encrypted tablespace:

   a. `ALTER SYSTEM SET ENCRYPTION KEY IDENTIFIED BY "<PASSWORD>"`

   b.
   ```
   CREATE TABLESPACE <TABLESPACE_NAME> EXTENT MANAGEMENT
   LOCAL AUTOALLOCATE SEGMENT SPACE MANAGEMENT AUTO DATAFILE
   '<DATA_FILE_LOCATION>' SIZE 100M AUTOEXTEND ON NEXT 50M
   MAXSIZE UNLIMITED ENCRYPTION DEFAULT STORAGE(ENCRYPT);
   ```

   Note: For `ENCRYPTION` parameter, you can choose to use `DEFAULT` or specify any other option.

After setting up Transparent Data Encryption (TDE) for Oracle Access Management, run the Oracle Fusion Middleware Repository Creation Utility (RCU) to create Oracle Access Management schemas. For more information, see Section 3.2.3, "Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU)".

Note: When you create the Oracle Access Management schemas using RCU, in the Map Tablespaces screen, use the tablespace that you created for Oracle Access Management in step 3b.

For more information, see "Map Tablespaces" topic in the *Oracle Fusion Middleware Repository Creation Utility User's Guide*.

6.5 Oracle Access Management in a New WebLogic Domain

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

It includes the following sections:

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure

6.5.1 Appropriate Deployment Environment

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

6.5.2 Components Deployed

Performing the configuration in this section deploys the following Oracle Access Management components:

- Oracle Access Manager
- Oracle Access Management Security Token Service
- Oracle Access Management Identity Federation
- Oracle Access Management Mobile and Social

6.5.3 Dependencies

The configuration in this section depends on the following:

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

6.5.4 Procedure

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

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

   The Oracle Fusion Middleware Configuration Wizard appears.

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

3. On the Select Domain Source screen, ensure that the **Generate a domain configured automatically to support the following products:** option is selected.

Select **Oracle Access Management - 11.1.2.0.0 [IAM_Home]**, and click **Next**. The Specify Domain Name and Location screen appears.

Note: When you select the **Oracle Access Management - 11.1.2.0.0 [IAM_Home]** option, the following options are also selected, by default:

- **Oracle Platform Security Service 11.1.1.0 [IAM_Home]**
- **Oracle JRF 11.1.1.0 [oracle_common]**

---

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

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

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

---

11. Optional: Configure Clusters, as required.

    For more information about configuring clusters for Oracle Identity and Access Management products, see the "Configuring High Availability for Oracle Identity and Access Management Components" topic in *Oracle Fusion Middleware High Availability Guide*.
12. Optional: Assign Managed Servers to clusters, as required.

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

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

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

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

15. Assign the newly created Managed Server, such as `oam_server1`, to a machine.

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

A new WebLogic domain to support Oracle Access Management 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.

Notes:

- After configuring Oracle Access Management in a new WebLogic administration domain, you must complete the procedure described in the following sections, before starting the servers:
  - Section 3.2.9, "Upgrading OPSS Schema using Patch Set Assistant"
  - Section 3.2.10, "Configuring Database Security Store for an Oracle Identity and Access Management Domain"
- After you configure Oracle Access Management, only Oracle Access Manager is enabled by default. To enable other Oracle Access Management components, such as OSTS, OIF, and Oracle Access Management Mobile and Social, refer to "Enabling or Disabling Available Services" topic in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.

6.6 Starting the Servers

After installing and configuring Oracle Access Management, you must run the Oracle WebLogic Administration Server and various Managed Servers, as described in Appendix C.1, "Starting the Stack". Ensure that you start the Oracle Access Management Administration Server before starting the Managed Servers.

6.7 Optional Post-Installation Tasks

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

- Configure your own LDAP to use instead of the default embedded LDAP, which comes with Oracle WebLogic Server.
- Configure a policy store to protect resources.

- Add more Managed Servers to the existing domain.
- Add a Managed Server instance.

For more information, see the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.

6.8 Verifying the Oracle Access Management Installation

After completing the installation process, including post-installation steps, you can verify the installation and configuration of Oracle Access Management 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 Management using the URL: `http://<adminserver-host>:<adminserver-port>/oamconsole`

   You will be redirected to `http://<oamserver-host>:<oamserver-port>/oam/server`.

   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 Management is successful, this console shows the Administration Server in running mode.

6.9 Setting Up Oracle Access Manager Agents

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

6.10 Setting Up Integration with OIM

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

6.11 Getting Started with Oracle Access Management After Installation

After installing Oracle Access Management, refer to the "Getting Started with Common Administration and Navigation" chapter in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.

Note: When you configure Oracle Access Management using the Oracle Access Management template, only Oracle Access Manager is enabled by default. For enabling other services including Security Token Service, Identity Federation, and Oracle Access Management Mobile and Social, refer to "Enabling or Disabling Available Services" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.

7

Configuring Oracle Adaptive Access Manager

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

- Overview
- Important Note Before You Begin
- Installation and Configuration Roadmap for Oracle Adaptive Access Manager
- Oracle Adaptive Access Manager in a New WebLogic Domain
- Configuring Oracle Adaptive Access Manager (Offline)
- Starting the Servers
- Post-Installation Steps
- Verifying the Oracle Adaptive Access Manager Installation
- Getting Started with Oracle Adaptive Access Manager After Installation

7.1 Overview

For Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0), Oracle Adaptive Access Manager includes two components:

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

> **Note:** Oracle Adaptive Access Manager (Offline) is included in the Oracle Identity and Access Management Suite. When you are installing Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0), Oracle Adaptive Access Manager (Offline) is also installed along with Oracle Adaptive Access Manager. For configuring Oracle Adaptive Access Manager (Offline), see Section 7.5, "Configuring Oracle Adaptive Access Manager (Offline)".

7.2 Important Note Before You Begin

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

Oracle Identity Navigator, Oracle Privileged Account Manager, and Oracle Access Management Mobile and Social. You can specify any name for this Oracle Home directory.

7.3 Installation and Configuration Roadmap for Oracle Adaptive Access Manager

Table 7–1 lists the tasks for installing and configuring Oracle Adaptive Access Manager.

Table 7–1 Installation and Configuration Flow for Oracle Adaptive Access Manager

No.	Task	Description
1	Review installation concepts in the Installation Planning Guide.	Read the *Oracle Fusion Middleware Installation Planning Guide*, which describes the process for various users to install or upgrade to Oracle Fusion Middleware 11*g* (11.1.2) depending on the user's existing environment.
2	Review the system requirements and certification documents to ensure that your environment meets the minimum installation requirements for the components you are installing.	For more information, see Section 2.1, "Reviewing System Requirements and Certification".
3	Obtain the Oracle Fusion Middleware Software.	For more information, see Section 3.2.1, "Obtaining the Oracle Fusion Middleware Software"
4	Review the Database requirements.	For more information, see Section 3.2.2, "Database Requirements".
5	Run Oracle Fusion Middleware Repository Creation Utility (RCU) to create and load the appropriate schemas for Oracle Identity and Access Management products.	For more information, see Section 3.2.3, "Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU)".
6	Review WebLogic Server and Middleware Home requirements.	For more information, see Section 3.2.4, "WebLogic Server and Middleware Home Requirements".
7	Start the Oracle Identity and Access Management Installer.	For more information, see Section 3.2.6, "Starting the Oracle Identity and Access Management Installer".
8	Install the Oracle Identity and Access Management 11*g* software.	Oracle Adaptive Access Manager is included in the Oracle Identity and Access Management Suite. You can use the Oracle Identity and Access Management 11*g* Installer to install Oracle Identity and Access Management Suite. For more information, see Section 3.2.7, "Installing Oracle Identity and Access Management 11g Release 2 (11.1.2.2.0)".
9	Run the Oracle Fusion Middleware Configuration Wizard to configure your Oracle Identity and Access Management products in a new or existing WebLogic domain.	This chapter describes the following configuration scenarios: ■ Section 7.4, "Oracle Adaptive Access Manager in a New WebLogic Domain" ■ Section 7.5, "Configuring Oracle Adaptive Access Manager (Offline)"
10	Upgrade the OPSS schema using Patch Set Assistant	For more information, see Section 3.2.9, "Upgrading OPSS Schema using Patch Set Assistant"

Table 7–1 (Cont.) Installation and Configuration Flow for Oracle Adaptive Access

No.	Task	Description
11	Configure the Database Security Store.	For more information, see Section 3.2.10, "Configuring Database Security Store for an Oracle Identity and Access Management Domain".
12	Start the servers.	You must start the Administration Server and all Managed Servers. For more information, see Section 7.6, "Starting the Servers".
13	Complete the post-installation tasks.	Complete the following post-installation tasks: ■ Section 7.7, "Post-Installation Steps" ■ Section 7.8, "Verifying the Oracle Adaptive Access Manager Installation" ■ Section 7.9, "Getting Started with Oracle Adaptive Access Manager After Installation"

7.4 Oracle Adaptive Access Manager in a New WebLogic Domain

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

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure

7.4.1 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 and Access Management 11*g* components, such as Oracle Identity Navigator, Oracle Access Management, or Oracle Identity Manager at a later time in the same domain.

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

7.4.2 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 on the Administration Server.

7.4.3 Dependencies

The configuration in this section depends on the following:

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

- Database schemas for Oracle Adaptive Access Manager. For more information, see Section 3.2.3, "Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU)".

7.4.4 Procedure

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

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

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

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

3. On the Select Domain Source screen ensure that the **Generate a domain configured automatically to support the following products:** option is selected. Select **Oracle Adaptive Access Manager Admin Server - 11.1.2.0.0 [IAM_Home]**.

   In addition, you can select the following:

   - **Oracle Adaptive Access Manager - Server - 11.1.2.0.0 [IAM_Home]**
   - **Oracle Adaptive Access Manager Offline - 11.1.2.0.0 [IAM_Home]**

   Note: When you select the **Oracle Adaptive Access Manager Admin Server - 11.1.2.0.0 [IAM_Home]** option, the following options are also selected, by default:

   - **Oracle Enterprise Manager 11.1.1.0 [oracle_common]**
   - **Oracle Platform Security Service 11.1.1.0 [IAM_Home]**
   - **Oracle JRF 11.1.1.0 [oracle_common]**

   When you select the **Oracle Adaptive Access Manager - Server - 11.1.2.0.0 [IAM_Home]** option, in addition to the templates mentioned above, the **Oracle WSM Policy Manager - 11.1.1.0 [oracle_common]** is also selected, by default.

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

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

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

6. The Configure Server Start Mode and JDK screen appears. Choose a JDK from the **Available JDKs** and select a **WebLogic Domain Startup Mode**. Click **Next**.

7. On the Configure JDBC Component Schema screen, select a component schema, such as the **OAAM Admin Server Schema**, the **OPSS Schema**, or the **OAAM Admin MDS Schema**, that you want to modify.

   You can set values for Schema Owner, Schema Password, Database and Service, Host Name, and Port. Click **Next**. The Test JDBC Component Schema screen

appears. After the test succeeds, click **Next**. The Select Optional Configuration screen appears.

8. On the Select Optional Configuration screen, you can configure the **Administration Server** and **Managed Servers, Clusters, and Machines**, and **Deployments and Services,** and **RDBMS Security Store**. Click **Next**.
9. Optional: Configure the following Administration Server parameters:
   - Name
   - Listen address
   - Listen port
   - SSL listen port
   - SSL enabled or disabled
10. On the Select Optional Configuration screen, select **Managed Servers, Clusters and Machines** to configure the managed server. For more information, see "Configure Managed Servers" in the *Oracle Fusion Middleware Creating Domains Using the Configuration Wizard*.
11. Optional: Configure Clusters, as required.

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

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

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

Note: After configuring Oracle Adaptive Access Manager in a new WebLogic administration domain, you must complete the procedure described in the following sections, before starting the servers:

- Section 3.2.9, "Upgrading OPSS Schema using Patch Set Assistant"
- Section 3.2.10, "Configuring Database Security Store for an Oracle Identity and Access Management Domain"

7.5 Configuring Oracle Adaptive Access Manager (Offline)

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

- Components Deployed
- Dependencies
- Procedure

7.5.1 Components Deployed

Performing the configuration in this section deploys the following:

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

7.5.2 Dependencies

The configuration in this section depends on the following:

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

7.5.3 Procedure

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

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

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

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

3. On the Select Domain Source screen, ensure that the **Generate a domain configured automatically to support the following products:** option is selected. Select **Oracle Adaptive Access Manager Offline - 11.1.2.0.0 [IAM_Home]**.

   Note: When you select the **Oracle Adaptive Access Manager Offline - 11.1.2.0.0 [IAM_Home]** option, the following options are also selected, by default:

   - **Oracle Enterprise Manager 11.1.1.0 [oracle_common]**
   - **Oracle Platform Security Service 11.1.1.0 [IAM_Home]**
   - **Oracle JRF 11.1.1.0 [oracle_common]**

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

4. Enter a name and a location for the domain to be created, and click **Next**. The Configure Administrator User Name and Password screen appears.
5. Configure a user name and a password for the administrator. The default user name is `weblogic`. Click **Next**. The Configure Server Start Mode and JDK screen appears.
6. Choose a JDK and **Production Mode** in the Configure Server Start Mode and JDK screen. Click **Next**. The Configure JDBC Component Schema screen is displayed.
7. On the Configure JDBC Component Schema screen, select a component schema, such as the **OAAM Offline Schema**, the **OPSS Schema**, or the **OAAM Admin MDS Schema** that you want to modify. You can set values for Schema Owner, Schema Password, Database and Service, Host Name, and Port. Click **Next**. The Test JDBC Component Schema screen appears. After the test succeeds, click **Next**. The Select Optional Configuration screen appears.
8. On the Select Optional Configuration screen, you can configure the **Administration Server**, **Managed Servers**, **Clusters**, **Machines**, **Deployments and Services**, and **RDBMS Security Store**. Select the relevant check boxes and click **Next**.
   - Optional: Configure the following Administration Server parameters:
     - Name
     - Listen Address
     - Listen Port
     - SSL Listen Port
     - SSL Enabled
   - Optional: Add and configure Managed Servers, as required. Note that Oracle Entitlements Server does not require a Managed Server because the application is deployed on the WebLogic Administration Server.
   - Optional: Configure Clusters, as required.

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

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

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

UNIX, the domain is created in the `<MW_HOME>/user_projects/domains` directory.

Note: After configuring Oracle Adaptive Access Manager in a new WebLogic administration domain, you must complete the procedure described in the following sections, before starting the servers:

- Section 3.2.9, "Upgrading OPSS Schema using Patch Set Assistant"
- Section 3.2.10, "Configuring Database Security Store for an Oracle Identity and Access Management Domain"

7.6 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 Appendix C.1, "Starting the Stack". Ensure that you start the Oracle Adaptive Access Manager Administration Server before starting the Managed Servers.

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

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

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

   - Challenge questions for English (United States)

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

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

- Entity definitions

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

- Out-of-the-box patterns

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

- Out-of-the-box configurable actions

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

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

- Out-of-the-box policies

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

- Any groups

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

  Notes:

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

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

- Default questions are shipped in the `oaam_kba_questions_<locale>.zip` files, which are located in the *<MW_HOME>*`/`*<IAM_ORACLE_HOME>*`/oaam/init/kba_questions` directory. The locale identifier <locale> specifies the language version.

- Base policies are shipped in the `oaam_sample_policies_for_uio_integration.zip` file, which is located in the *<MW_HOME>/<IAM_ORACLE_HOME>*`/oaam/init` directory.
- Configurable action templates are shipped in the `OOTB_Configurable_Actions.zip` file, which is located in the *<MW_HOME>/<IAM_ORACLE_HOME>*`/oaam/init` directory.
- Base-authentication required entities are shipped in the `Auth_EntityDefinition.zip` file, which is located in the *<MW_HOME>/<IAM_ORACLE_HOME>*`/oaam/init` directory.

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

4. Load Location Data into the Oracle Adaptive Access Manager database as follows:
   a. Configure the IP Location Loader script, as described in the topics "OAAM Command Line Interface Scripts" and "Importing IP Location Data" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*.
   b. Make a copy of the `sample.bharosa_location.properties` file, which is located under the `<MW_HOME>/<IAM_Home>/oaam/cli` directory (on UNIX). On Windows, the `sample.bharosa_location.properties` file is located under the `<MW_HOME>\<IAM_Home>\oaam\cli` directory.

      Enter location data details in the `location.data` properties, as in the following examples:

      On Windows:

      ```
      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
      ```

      On UNIX:

      ```
      location.data.provider=quova

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

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

      location.data.anonymizer.file=/tmp/quova/anonymizers_2008-07-09.dat.gz
      ```

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

      On Windows: `loadIPLocationData.cmd`

      On UNIX: `./loadIPLocationData.sh`

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

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

7.8 Verifying the Oracle Adaptive Access Manager Installation

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

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

     ```
     <MW_HOME>\user_projects\domains\base_
     domain\bin\startWebLogic
     ```

   - On UNIX: At the $ prompt, run the `startWebLogic.sh` script to start the Administration Server, as in the following example:

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

2. Start the Managed Server, as described in Section 7.6, "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 admin server username and password. Log in to the Administration Server using the following URL:

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

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

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

5. Log in to the Oracle Adaptive Access Manager Offine Server using the following URL:

   ```
   https://<host>:<oaam_offline_server1_port>/oaam_offline
   ```

7.9 Getting Started with Oracle Adaptive Access Manager After Installation

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

8

Installing and Configuring Oracle Entitlements Server

This chapter describes how to install and configure Oracle Entitlements Server 11*g* Release 2 (11.1.2.2.0).

It discusses the following topics:

- Important Note Before You Begin
- Overview of Oracle Entitlements Server 11g Installation
- Installation and Configuration Roadmap for Oracle Entitlements Server
- Configuring Oracle Entitlements Server Administration Server
- Installing Oracle Entitlements Server Client
- Configuring Oracle Entitlements Server Client
- Getting Started with Oracle Entitlements Server After Installation

8.1 Important Note Before You Begin

Before you start installing and configuring Oracle Entitlements Server, ensure that you have reviewed the information provided in Part I, "Introduction and Preparation".

Note that **IAM_HOME** is used to refer to the Oracle Home directory that includes Oracle Identity Manager, Oracle Access Management, Oracle Adaptive Access Manager, Oracle Entitlements Server, Oracle Identity Navigator, Oracle Privileged Account Manager, and Oracle Access Management Mobile and Social. You can specify any name for this Oracle Home directory.

8.2 Overview of Oracle Entitlements Server 11*g* Installation

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

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

- Oracle Entitlements Server Administration Server
- Oracle Entitlements Server Client (Security Module)

Oracle Entitlements Server Administration Server

This component is included in the Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0) installation. The Administration Server manages the storage of policy data in the database and the transactional distribution of policies to the Security Modules.

Oracle Entitlements Server Client (Security Module)

This component has its own installer and it is not included in the Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0) installation. The Oracle Entitlements Server Client does not require Oracle WebLogic Server.

8.3 Installation and Configuration Roadmap for Oracle Entitlements Server

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

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

No.	Task	Description
1	Review installation concepts in the Installation Planning Guide.	Read the *Oracle Fusion Middleware Installation Planning Guide*, which describes the process for various users to install or upgrade to Oracle Fusion Middleware 11*g* (11.1.2) depending on the user's existing environment.
2	Review the system requirements and certification documents to ensure that your environment meets the minimum installation requirements for the components you are installing.	For more information, see Section 2.1, "Reviewing System Requirements and Certification".
3	Obtain the Oracle Fusion Middleware Software.	For more information, see Section 3.2.1, "Obtaining the Oracle Fusion Middleware Software"
4	Review the Database requirements.	Oracle recommends that you install Oracle Database. For more information, see Section 3.2.2, "Database Requirements".
5	Create and load the appropriate schemas for Oracle Entitlements Server.	Depending on the policy store you choose for Oracle Entitlements Server, complete one of the following: ■ If you are using Oracle Database for Oracle Entitlements Server policy store, then you must create schemas for Oracle Entitlements Server using the Oracle Fusion Middleware Repository Creation Utility (RCU). For more information, see Section 3.2.3, "Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU)". ■ Apache Derby 10.5.3.0, an evaluation database is included in your Oracle WebLogic Server installation. If you are using Apache Derby for Oracle Entitlements Server policy store, you must create schemas for Oracle Entitlements Server as described in Appendix H, "Creating Oracle Entitlement Server Schemas for Apache Derby".
6	Review WebLogic Server and Middleware Home requirements.	For more information, see Section 3.2.4, "WebLogic Server and Middleware Home Requirements".
7	Start the Oracle Identity and Access Management Installer.	For more information, see Section 3.2.6, "Starting the Oracle Identity and Access Management Installer".

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

No.	Task	Description
8	Install the Oracle Identity and Access Management 11*g* software.	Oracle Entitlements Server is included in the Oracle Identity and Access Management Suite. You can use the Oracle Identity and Access Management 11*g* Installer to install Oracle Identity and Access Management Suite. For more information, see Section 3.2.7, "Installing Oracle Identity and Access Management 11g Release 2 (11.1.2.2.0)".
9	Run the Oracle Fusion Middleware Configuration Wizard to configure Oracle Entitlements Server Administration Server.	For more information, see Section 8.4, "Configuring Oracle Entitlements Server Administration Server".
10	Install the Oracle Entitlements Server Client software.	For more information, see Section 8.5, "Installing Oracle Entitlements Server Client".
11	Configure Oracle Entitlements Server Client.	For more information, see Section 8.6, "Configuring Oracle Entitlements Server Client".
12	Get started with Oracle Entitlements Server.	For more information, see Section 8.7, "Getting Started with Oracle Entitlements Server After Installation".

8.4 Configuring Oracle Entitlements Server Administration Server

This topic describes how to configure Oracle Entitlements Server in a new WebLogic domain. It includes the following sections:

- Components Deployed
- Extracting Apache Derby Template (Optional)
- Configuring Oracle Entitlements Server in a New WebLogic Domain
- Upgrading OPSS Schema using Patch Set Assistant
- Configuring Security Store for Oracle Entitlements Server Administration Server
- Starting the Servers
- Verifying Oracle Entitlements Server Configuration

8.4.1 Components Deployed

Performing the configuration in this section deploys the following:

- WebLogic Administration Server
- Oracle Entitlements Server application on the Administration Server

8.4.2 Extracting Apache Derby Template (Optional)

If you are using Apache Derby, then you must extract the `oracle.apm_11.1.1.3.0_template_derby.zip` file (located in `IAM_HOME/common/templates/applications`) and save `oracle.apm_11.1.1.3.0_template_derby.jar` file to the following location:

```
IAM_HOME\common\templates\applications
```

8.4.3 Configuring Oracle Entitlements Server in a New WebLogic Domain

Perform the following steps to configure Oracle Entitlements Server in a new WebLogic domain:

1. Run the `IAM_HOME/common/bin/config.sh` script (on UNIX), or `IAM_HOME\common\bin\config.cmd` (on Windows).

   The Fusion Middleware Configuration Wizard appears.

2. On the Welcome screen, select the **Create a new WebLogic domain** option. Click **Next**.

   The Select Domain Source screen appears.

3. On the Select Domain Source screen, ensure that the **Generate a domain configured automatically to support the following products:** option is selected.

   Select one of the following options:

   - **Oracle Entitlements Server for Admin Server- 11.1.1.0 [IAM_HOME]**
   - **Oracle Entitlements Server for Managed Server- 11.1.1.0 [IAM_HOME]**

   Notes:

   - If you select the **Oracle Entitlements Server for Admin Server- 11.1.1.0 [IAM_HOME]** option, the following options are also selected, by default:
     - **Oracle Platform Security Service 11.1.1.0 [IAM_HOME]**
     - **Oracle JRF 11.1.1.0 [oracle_common]**
   - If you select the **Oracle Entitlements Server for Managed Server- 11.1.1.0 [IAM_HOME]** option, the following options are also selected, by default:
     - **Oracle Platform Security Service 11.1.1.0 [IAM_HOME]**
     - **Oracle JRF 11.1.1.0 [oracle_common]**
   - If you using Apache Derby, then select the **Oracle Entitlements Server Security Module - 11.1.1.0 [IAM_HOME]** option.

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

4. Enter a name and a location for the domain to be created, and click **Next**.

   The Configure Administrator User Name and Password screen appears.

5. Enter a user name and a password for the administrator. The default user name is `weblogic`. Click **Next**.

   Note: When you enter the user name and the password for the administrator, be sure to remember them. This is the WebLogic Administrator user name and password that you must specify for logging in to the WebLogic Server Administration Console. The Oracle WebLogic Server Administration Console is a Web browser-based, graphical user interface that you use to manage a WebLogic Server domain.

   The Configure Server Start Mode and JDK screen appears.

6. Choose a JDK from the **Available JDKs** and then select a **WebLogic Domain Startup Mode**. Click **Next**.

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

   The Configure JDBC Component Schema screen is displayed.

7. On the Configure JDBC Component Schema screen, select the **Oracle Entitlements Server Schema** and specify the Schema Owner, Schema Password, DBDS/Service, Host Name, and Port.

   Note: The Schema Owner refers to the name that you specified when creating the database schemas for Oracle Entitlements Server using the Oracle Fusion Middleware Repository Creation Utility (RCU).

   For Database related information, refer to the `tnsnames.ora` file (located in the *`DB_INSTALL_DIR`*`/product/11.2.0/`*`DB_INSTANCE`*`/network/admin` directory, where *`DB_INSTALL_DIR`* is the location where Oracle Database was installed, and *`DB_INSTANCE`* by default is `dbhome_1)`.

   Click **Next**. The Test JDBC Component Schema screen appears.

8. Select the component schema you want to test, and click **Test Connections**. After the test succeeds, click **Next**. If the test fails, click **Previous**, correct the values that you entered in step 7, and test the connection again.

   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**.

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

11. The Creating Domain screen appears. This screen shows the progress of the domain creation. When the domain creation process completes, this screen displays the Domain location and the Admin Server URL.

    After reviewing the information displayed on the screen, click **Done** to close the Configuration Wizard.

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

8.4.4 Upgrading OPSS Schema using Patch Set Assistant

You must upgrade the Oracle Platform Security Services (OPSS) schema that you had created using the RCU in Section 3.2.3, "Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU)".

To upgrade the schemas, complete the following steps:

- Starting Patch Set Assistant

- Using the Patch Set Assistant Graphical Interface
- Verifying Schema Upgrade

8.4.4.1 Starting Patch Set Assistant

To start Patch Set Assistant, do the following:

On UNIX:

1. Move from your present working directory to the *MW_HOME*/oracle_common/bin directory by running the following command on the command line:

   ```
   cd <MW_HOME>/oracle_common/bin
   ```

2. Run the following command:

   ```
   ./psa
   ```

On Windows:

1. Move from your present working directory to the *MW_HOME*\oracle_common\bin directory by running the following command on the command line:

   ```
   cd <MW_HOME>\oracle_common\bin
   ```

2. Execute the following command:

   ```
   psa.bat
   ```

8.4.4.2 Using the Patch Set Assistant Graphical Interface

After starting the Patch Set Assistant Installer, follow the instructions in Table 8–2 to update your schemas.

Table 8–2 Patch Set Assistant Screens

Screen	Description
Welcome	This page introduces you to the Patch Set Assistant.
Select Component	Select the **Oracle Platform Security Services** schema. **NOTE:** Do not select any other components that are listed on the Select Component screen.
Prerequisite	Verify that you have satisfied the database prerequisites.
Schema	Specify your database credentials to connect to your database, then select the schema you want to update. Note that this screen appears once for each schema that must be updated as a result of the component you selected on the Select Component screen.
Examine	This page displays the status of the Patch Set Assistant as it examines each component schema. Verify that your schemas have a "successful" indicator in the Status column.
Upgrade Summary	Verify that the schemas are the ones you want to upgrade.
Upgrade Progress	This screen shows the progress of the schema upgrade.
Upgrade Success	Once the upgrade is successful, this screen is displayed.

8.4.4.3 Verifying Schema Upgrade

You can verify the schema upgrade by checking out the log files. The Patch Set Assistant writes log files in the following locations:

On UNIX:

MW_HOME/oracle_common/upgrade/logs/psa/psatimestamp.log

On Windows:

MW_HOME\oracle_common\upgrade\logs\psa\psatimestamp.log

Some components create a second log file named `psatimestamp.out` in the same location.

The `timestamp` reflects the actual date and time when Patch Set Assistant was run.

If any failures occur when running Patch Set Assistant, you can use these log files to help diagnose and correct the problem. Do not delete them. You can alter the contents of the log files by specifying a different `-logLevel` from the command line.

Some of the operations performed by Patch Set Assistant may take longer to complete than others. If you want to see the progress of these long operations, you can see this information in the log file, or you can use the following query:

```
SELECT VERSION, STATUS, UPGRADED FROM SCHEMA_VERSION_REGISTRY WHERE OWNER='schema_
name';
```

In the query results, the `STATUS` field is either `UPGRADING` or `UPGRADED` during the schema patching operation, and becomes `VALID` when the operation is completed.

After running the Patch Set Assistant, the Oracle Platform Security Services schema version should be 11.1.1.7.2.

8.4.5 Configuring Security Store for Oracle Entitlements Server Administration Server

You must run the `configureSecurityStore.py` script to configure the security store for Oracle Entitlements Server Administration Server. Security store is a repository of system and application-specific policies, credentials, and keys.

The `configureSecurityStore.py` script is located in the `<IAM_HOME>\common\tools` directory. You can use the `-h` option for help information about using the script.

Configure the security store for Oracle Entitlements Server Administration Server as follows:

On Windows:

```
<MW_HOME>\oracle_common\common\bin\wlst.cmd <IAM_
HOME>\common\tools\configureSecurityStore.py -d <domaindir> -s
<datasource> -f <farmname> -t <servertype> -j <jpsroot> -m
<mode> -p <password>
```

For example:

```
<MW_HOME>\oracle_common\common\bin\wlst.cmd <IAM_
HOME>\common\tools\configureSecurityStore.py -d <MW_Home>\user_
projects\domains\base_domain -t DB_ORACLE -j cn=jpsroot -m
create -p welcome1
```

For an example of the `join` option, see "Configuring the Database Security Store Using the Join Option".

On UNIX:

```
<MW_HOME>/oracle_common/common/bin/wlst.sh <IAM_
HOME>/common/tools/configureSecurityStore.py -d <domaindir> -s
```

```
<datasource> -f <farmname> -t <servertype> -j <jpsroot> -m
<mode> -p <password>
```

For example:

```
<MW_HOME>/oracle_common/common/bin/wlst.sh <IAM_
HOME>/common/tools/configureSecurityStore.py -d <MW_Home>/user_
projects/domains/base_domain -t DB_ORACLE -j cn=jpsroot -m
create -p welcome1
```

For an example of the `join` option, see "Configuring the Database Security Store Using the Join Option".

Table 8–3 describes the parameters that you may specify on the command line.

Table 8–3 OES Administration Server Security Store Configuration Parameters

Parameter	Description
`-d` *domaindir*	Location of the Oracle Entitlements Server Administration Server Domain.
`-s` *datasource*	The data source of security store configured in domain. It is optional, default value is `opss-DBDS`.
`-f` *farmname*	The security store farm name. It is optional, default value is the domain name.
`-t` *servertype*	The policy store type. For example: `DB_ORACLE`, `DB_DERBY`, or `OID`. It is optional, default value is `DB_ORACLE`.
`-j` *jpsroot*	The distinguished name of jpsroot. It is optional, default value is `cn=jpsroot`.
`-m` *mode*	`create`- Use `create` if you want to create a new database security store. `join`- Use `join` if you want to use an existing database security store for the domain. `validate`- Use `validate` to verify whether the Security Store has been configured correctly. This command validates diagnostics data created during initial creation of the Security Store. `validatefix`- Use `validatefix` to fix diagnostics data present in the Security Store. `fixjse`- Use `fixjse` to update the domain's Database Security Store credentials used for access by JSE tools.

Table 8–3 (Cont.) OES Administration Server Security Store Configuration Parameters

Parameter	Description
`-c config`	The configuration mode of the domain. For example: `IAM`. It is optional, default value is `None`. **Note:** If `-c <config>` option is specified, OES Admin Server will be configured in mixed mode, then it can only distribute policies to Security Modules in non-controlled mode and controlled pull mode. For example: If the OES Administration Server is deployed in the domain where other Oracle Identity and Access Management components (OIM, OAM, OAAM, OPAM, or OIN) are deployed, then the domain is configured in mixed mode. In this case, the OES Administration Server is used for managing the Oracle Identity and Access Management policies only. It should not be used to manage the policies for any other applications protected by OES Security Modules. If `-c <config>` option is not specified, OES Admin Server will be configured in non-controlled mode, it can distribute policies to Security Modules in controlled push mode. For example: If you want to use OES Administration Server to manage custom applications which are protected by OES Security Modules, then the OES Administration Server must be deployed in a domain with non-controlled distribution mode.
`-p password`	The OPSS schema password.
`-k keyfilepath`	The directory containing the encryption key file `ewallet.p12`. If `-m join` is specified, this option is mandatory.
`-w keyfilepassword`	The password used when the domain's key file was generated. If `-m join` is specified, this option is mandatory.
`-u username`	The user name of the OPSS schema. If `-m fixjse` is specified, this option is mandatory.

8.4.6 Starting the Servers

After installing and configuring Oracle Entitlements Server, you must start the Administration Server and the Managed Server based on the option that you had selected on the **Select Domain Source** screen of the Oracle Fusion Middleware Configuration Wizard. For more information, see Appendix C.1, "Starting the Stack".

Ensure that you start the Oracle Entitlements Server Administration Server before starting the Managed Server.

8.4.7 Verifying Oracle Entitlements Server Configuration

- To verify that your Oracle Entitlements Server Administration Server configuration was successful, use the following URL to log in to the Oracle Entitlements Server Administration Console:

  `http://hostname:port/apm/`

Where `hostname` is the DNS name or IP address of the Administration Server and `port` is the address of the port on which the Administration Server listens for requests. You can obtain these values from the `AdminServer.log` file.

The `AdminServer.log` file is located in the `MW_HOME/user_projects/domains/domain_name/servers/AdminServer/logs` directory (on UNIX) or the `MW_HOME\user_projects\domains\domain_name\servers\AdminServer\logs` directory (on Windows).

- To verify that your Oracle Entitlements Server Managed Server configuration was successful, use the following URL:

  `http://<oes_server1-hostname>:<oes_server1-port>/apm/`

For more information, see the section "Logging In to and Signing Out of the User Interface" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Entitlements Server*.

8.5 Installing Oracle Entitlements Server Client

This section contains the following topic:

- Prerequisites
- Obtaining Oracle Entitlements Server Client Software
- Installing Oracle Entitlements Server Client
- Verifying Oracle Entitlements Server Client Installation
- Applying a Patch Using OPatch

8.5.1 Prerequisites

Before installing the Oracle Entitlements Server Client software, ensure that you have installed and configured the Oracle Entitlements Server Administration Server.

8.5.2 Obtaining Oracle Entitlements Server Client Software

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

8.5.3 Installing Oracle Entitlements Server Client

To install Oracle Entitlements Server Client, extract the contents of `oesclient.zip` to your local directory and then start the Installer by executing one of the following commands:

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

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

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

```
<full path to the setup.exe directory>\setup.exe
-jreLoc C:\MW_HOME\jdk\jre
```

You must specify the `-jreLoc` option on the command line when using the JDK to avoid installation issues.

Follow the instructions in Table 8–4 to install Oracle Entitlements Server Client.

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

Table 8–4 Installation Flow for the Oracle Entitlements Server Client

No.	Screen	Description and Action Required
1	Welcome	Click **Next** to continue.
2	Prerequisite Checks	If all prerequisite checks pass inspection, then click **Next** to continue.
3	Specify Installation Location	In the **Oracle Home Directory** field, enter the directory where you want to install the Oracle Entitlements Server client. This directory is also referred to as `OES_CLIENT_HOME` in this book. **Note:** If the Security Module you want to configure requires creation or extension of a WebLogic domain, then you must install the Oracle Entitlements Server client in the Middleware Home that was created during WebLogic Server installation. This applies to the following Security Module configurations: ■ WebLogic Server Security Module in a JRF environment ■ WebLogic Server Security Module in a Non-JRF environment ■ Web Service Security Module on Oracle WebLogic Server domain in a JRF environment ■ Web Service Security Module on Oracle WebLogic Server domain in a Non-JRF environment ■ Oracle Service Bus Security Module For the above Security Module configurations, Oracle recommends that you install the Oracle Entitlements Server client in a separate directory in the same Middleware Home where the Oracle Entitlements Server Administration server is installed. For example, `MW_HOME/OES_CLIENT_HOME`. For the other Security Modules, the `OES_CLIENT_HOME` can be any other directory where you want to install the Oracle Entitlements Server client. Click **Next** to continue.

Table 8–4 (Cont.) Installation Flow for the Oracle Entitlements Server Client

No.	Screen	Description and Action Required
4	Installation Summary	The Installation Summary Page screen displays a summary of the choices that you made. Review this summary and decide whether to start the installation. If you want to modify any of the configuration settings at this stage, select a topic in the left navigation page and modify your choices. Click **Save** to save the installation response file, which contains your responses to the Installer prompts and fields. To continue installing Oracle Entitlements Server Client, click **Install**.
5	Installation Progress	The Installation Progress screen appears. Monitor the progress of your installation. The location of the installation log file is listed for reference. Make a note of the name and location of the installation log file for your reference. After the installation progress reaches 100%, click **OK**. If you are installing on a UNIX system, you may be asked to run the *OES_CLIENT_HOME*`/oracleRoot.sh` script to set up the proper file and directory permissions.
8	Installation Complete	Click **Finish** to dismiss the installer. This installation process copies the OES Client software to your system and creates an `OES_CLIENT_HOME` directory in the location that you specified in step 3.

8.5.4 Verifying Oracle Entitlements Server Client Installation

To verify that your Oracle Entitlements Server Client installation is successful, go to your *OES_CLIENT_HOME* directory which you specified during installation, and verify that the *OES_CLIENT_HOME* directory is created and populated with product files.

You can also verify the installation log file that is generated after the installation is complete. The name and location of the installation log file is displayed on the Installation Progress screen (in step 5) of the Oracle Entitlements Server Client installation.

8.5.5 Applying a Patch Using OPatch

If you have installed the Oracle Entitlements Server Client software in a separate Middleware Home than the Oracle Entitlements Server Administration Server, then after installing the Oracle Entitlements Server Client software, you must apply a patch to the `oracle_common` directory using OPatch, as described in the steps below.

Note: Skip this step if you are installing the Oracle Entitlements Server Client software into the same Middleware Home as the Oracle Entitlements Server Administration Server, because it has already been applied automatically.

This patch applies only to the following Security Module configurations:

- WebLogic Server Security Module in a JRF environment
- Web Service Security Module on Oracle WebLogic Server domain in a JRF environment
- WebSphere Security Module in a JRF environment
- Oracle Service Bus Security Module

To apply a patch to `oracle_common` directory using OPatch, do the following:

1. Go to the `OES_CLIENT_HOME/oneoffpatches` directory.
2. Extract the contents of the `ENTSEC_OPSS_p17403853_111170_Generic.zip` file to a directory. By default, this directory is named `ENTSEC_OPSS_p17403853_111170_Generic`.
3. Go to the `OES_CLIENT_HOME/oneoffpatches/ENTSEC_OPSS_p17403853_111170_Generic` directory, and follow the instructions provided in the `README.txt` file.

8.6 Configuring Oracle Entitlements Server Client

Policy data is distributed in a *controlled* manner or in a *non-controlled* manner.

The distribution mode is defined in the `jps-config.xml` configuration file for each Security Module. The specified distribution mode is applicable for all Application Policy objects bound to that Security Module.

Note: Oracle recommends that you configure Oracle Entitlements Server Client in the *controlled* distribution mode. However, if you configure a Security Module in a JRF environment, then *non-controlled* distribution mode is the only supported distribution mode.

This section describes how to configure the following:

- Configuring Distribution Modes
- Configuring Security Modules in a Controlled Push Mode (Quick Configuration)
- Configuring Security Modules
- Locating Security Module Instances
- Using the Java Security Module
- Configuring the PDP Proxy Client

8.6.1 Configuring Distribution Modes

For introductory information about distribution modes, see the section "Defining Distribution Modes" in the *Oracle Fusion Middleware Developer's Guide for Oracle Entitlements Server*.

The following sections explains how to configure the distribution modes.

- Configuring Controlled Push Distribution Mode
- Configuring Non-Controlled and Controlled Pull Distribution Mode

8.6.1.1 Configuring Controlled Push Distribution Mode

To configure a controlled push distribution mode, open the `smconfig.prp` file (located in `OES_CLIENT_HOME/oessm/SMConfigTool`) in a text editor, and edit the following parameters described in Table 8–5.

Table 8–5 smconfig.prp File Parameters (Controlled Distribution)

Parameter	Description
`oracle.security.jps.runtime.pd.client.policyDistributionMode`	Accept the default value `controlled-push` as the distribution mode.
`oracle.security.jps.runtime.pd.client.RegistrationServerHost`	Enter the address of the Oracle Entitlements Server Administration Server.
`oracle.security.jps.runtime.pd.client.RegistrationServerPort`	Enter the SSL port number of the Oracle Entitlements Server Administration Server. You can find the SSL port number from the WebLogic Administration console.

8.6.1.2 Configuring Non-Controlled and Controlled Pull Distribution Mode

Open the `smconfig.prp` file (located in `OES_CLIENT_HOME/oessm/SMConfigTool`) in a text editor and edit the following parameters described in Table 8–6.

Table 8–6 smconfig.prp File Parameters Non- Controlled Distribution

Parameter	Description
`oracle.security.jps.runtime.pd.client.policyDistributionMode`	Enter non-`controlled` or `controlled-pull` as the distribution mode.
`oracle.security.jps.policystore.type`	Specify the policy store type. For example, `DB` for Oracle Database, `OID` for Oracle Internet Directory, and `Derby` for Apache Derby.
`jdbc.url`	If you are using database as the policy store, then specify your database policy store JDBC URL. For example, `jdbc:oracle:thin:@myhost:1521/orcl`
`ldap.url`	If you are using LDAP as the policy store, then specify your LDAP URL. For example, `ldap://myhost:port`
`oracle.security.jps.farm.name`	Specify your domain name. The default value is `cn=oes_domain`.
`oracle.security.jps.ldap.root.name`	Specify the root name of jps context. The default value is `cn=jpsroot`.

8.6.1.2.1 Setting Up Connection to an Oracle Database

If you are configuring a Non-Controlled or Controlled Pull Distribution Mode, then you must set up a connection to an Oracle Database. The procedure for setting up connection to an Oracle Database differs based on the type of Security Module you choose to configure.

This section includes the following topics:

- Setting Up Connection to an Oracle Database for Security Modules Configured in a Non-JRF Environment
- Setting Up Connection to an Oracle Database for Security Modules Configured in a JRF Environment

Setting Up Connection to an Oracle Database for Security Modules Configured in a Non-JRF Environment

If you configure a Security Module in a non-JRF environment, then you must complete the following steps for setting up a connection to an Oracle Database:

1. Create a JDBC Data Source using the WebLogic Server Administration Console. This data source is used to connect to the Policy Store of the OES Administration Server. For more information, see "Create JDBC generic data sources" topic in the *Oracle Fusion Middleware Oracle WebLogic Server Administration Console Online Help* document, available at the following link:

   `http://docs.oracle.com/cd/E23943_01/apirefs.1111/e13952/taskhelp/jdbc/jdbc_datasources/CreateDataSources.html`

   When you follow the instructions in the above link, then in step 7 you are required to enter a value for **Database User Name**. The value for this parameter must be same as the one you used when creating schemas for Oracle Entitlements Server using the Oracle Fusion Middleware Repository Creation Utility (RCU). For example, *prefix*_OPSS.

2. Open the `jps-config.xml` file located in *MW_HOME*`/user_projects/domains/`*Domain_Name*`/config/fmwconfig/AdminServer` directory (on UNIX), or *MW_HOME*`\user_projects\domains\`*Domain_Name*`\config\fmwconfig\AdminServer` directory (on Windows).

3. Locate `pdp.service` and replace the existing `jdbc.url` property with the following property:

   ```
   <property value="jdbc/OPSSDBDS" name="datasource.jndi.name"/>
   ```

   Note: *jdbc/OPSSDBDS* is the name of the JDBC datasource used for the OES.

4. Delete the following properties:
   - `jdbc.driver`
   - `jdbc.url`
   - `bootstrap.security.principal.key`
   - `bootstrap.security.principal.map`

5. Save the `jps-config.xml` file.

Setting Up Connection to an Oracle Database for Security Modules Configured in a JRF Environment

If you configure a Security Module in a JRF environment, then you must complete the following steps for setting up a connection to an Oracle Database:

1. Create a JDBC Data Source using the WebLogic Server Administration Console. This data source is used to connect to the Policy Store of the OES Administration Server. For more information, see "Create JDBC generic data sources" topic in the *Oracle Fusion Middleware Oracle WebLogic Server Administration Console Online Help* document, available at the following link:

   http://docs.oracle.com/cd/E23943_01/apirefs.1111/e13952/taskhelp/jdbc/jdbc_datasources/CreateDataSources.html

   When you follow the instructions in the above link, then in step 7 you are required to enter a value for **Database User Name**. The value for this parameter must be same as the one you used when creating schemas for Oracle Entitlements Server using the Oracle Fusion Middleware Repository Creation Utility (RCU). For example, *prefix*_OPSS.

2. Start the Oracle Entitlements Server Client domain. For more information, see Appendix C.1, "Starting the Stack".

3. Reassociate the policies using the WLST `reassociateSecurityStore` command, as follows:

   a. Start the WLST shell.

   ```
   cd ORACLE_HOME/common/bin
   ./wlst.sh
   ```

   b. Connect to the WebLogic Administration Server using the WLST connect command.

   ```
   connect ("AdminUser", "AdminPassword", "hostname:port")
   ```
   For example:
   ```
   connect ("weblogic", "welcome1", "ADMINHOST:7001")
   ```

   c. Run the `reassociateSecurityStore` command.

   ```
   reassociateSecurityStore(domain="OESDomain", servertype="DB_ORACLE",
   datasourcename="Datasource_Name", jpsroot="cn=reassociatedb", join="true")
   ```

   Note: The values for `domain` and `jpsroot` must be same as the value for `farmname` in the `jps-config.xml` file. This file is located in *MW_HOME*`/user_projects/domains/`*Domain_Name*`/config/fmwconfig` directory (on UNIX), or *MW_HOME*`\user_projects\domains\`*Domain_Name*`\config\fmwconfig` directory (on Windows)

   `datasourcename` is the name of the Data Source that you created in step 1.

4. Restart the Oracle Entitlements Server Client domain after the command completes successfully. For more information, see Appendix C.1, "Starting the Stack".

8.6.2 Configuring Security Modules in a Controlled Push Mode (Quick Configuration)

These section describes how to configure the Security Module quickly using pre-existing `smconfig.prp` files.

> **Note:** Security Module can be configured by running the `config.sh` command. This section describes how to configure various security modules in a controlled push mode.
>
> If the Administration Server configuration is using a customer digital certificate, you must use the parameter `-skipEnroll` when you run the `config.sh` command to configure security module.

- Configuring Java Security Module in a Controlled Push Mode
- Configuring RMI Security Module in a Controlled Push Mode
- Configuring Web Service Security Module in a Controlled Push Mode
- Configuring Oracle WebLogic Server Security Module in a Controlled Push Mode

8.6.2.1 Configuring Java Security Module in a Controlled Push Mode

To configure Java Security Module instance in a controlled distribution mode, do the following:

1. Open `smconfig.java.controlled.prp` file (located in, `OES_CLIENT_HOME/oessm/SMConfigTool`) in a text editor, and then specify the parameters described in Table 8–5.
2. Run the `config.sh` (located in `OES_CLIENT_HOME/oessm/bin` on UNIX) or `config.cmd` (located in `OES_CLIENT_HOME\oessm\bin` on Windows) as follows:

```
config.sh -smConfigId <SM_NAME> -prpFileName OES_CLIENT_
HOME/oessm/SMConfigTool/smcon
fig.java.controlled.prp
```

3. When prompted, specify the following:
   - New key store password for enrollment.
   - Oracle Entitlements Server user name (This is the Administration Server's user name).
   - Oracle Entitlements Server password (This is the Administration Server's password)

8.6.2.2 Configuring RMI Security Module in a Controlled Push Mode

To configure RMI Security Module instance in a controlled distribution mode, then do the following:

1. Open `smconfig.rmi.controlled.prp` file (located in `OES_CLIENT_HOME/oessm/SMConfigTool`) in a text editor, and then specify the parameters described in Table 8–5.
2. Run the `config.sh` (located in `OES_CLIENT_HOME/oessm/bin` on UNIX) or `config.cmd` (located in `OES_CLIENT_HOME\oessm\bin` on Windows) as follows:

```
config.sh -smConfigId <SM_NAME> -RMIListeningPort <RMISM_PORT> -prpFileName
```

```
OES_CLIENT_HOME/oessm/SMConfigTool/smconfig.rmi.controlled.prp
```

3. When prompted, specify the following:
   - New key store password for enrollment
   - Oracle Entitlements Server user name (This is the Administration Server's user name)
   - Oracle Entitlements Server Password (This is the Administration Server's password)

8.6.2.3 Configuring Web Service Security Module in a Controlled Push Mode

To configure Web Service Security Module instance in a controlled distribution mode, do the following:

1. Open `smconfig.ws.controlled.prp` file (located in `OES_CLIENT_HOME/oessm/SMConfigTool`) in a text editor, and then specify the parameters described in Table 8–5.
2. Run the `config.sh` (located in `OES_CLIENT_HOME/oessm/bin` on UNIX) or `config.cmd` (located in `OES_CLIENT_HOME\oessm\bin` on Windows) as follows:

   ```
   config.sh -smConfigId <SM_NAME> -WSListeningPort <WSSM_PORT> -prpFileName OES_
   CLIENT_HOME/oessm/SMConfigTool/smconfig.ws.controlled.prp
   ```

3. When prompted, specify the following:
   - New key store password for enrollment
   - Oracle Entitlements Server user name (This is the Administration Server's user name)
   - Oracle Entitlements Server password (This is the Administration Server's password)

8.6.2.4 Configuring Oracle WebLogic Server Security Module in a Controlled Push Mode

To configure Oracle WebLogic Server Security Module instance in a controlled distribution mode, do the following:

1. Open `smconfig.wls.controlled.prp` file (located in `OES_CLIENT_HOME/oessm/SMConfigTool`) in a text editor, and then specify the parameters described in Table 8–5.
2. Run the `config.sh` (located in `OES_CLIENT_HOME/oessm/bin` on UNIX) or `config.cmd` (located in `OES_CLIENT_HOME\oessm\bin` for Windows) as follows:

   ```
   config.sh -smConfigId <SM_NAME> -prpFileName $OES_CLIENT_
   HOME/oessm/SMConfigTool/smconfig.wls.controlled.prp -serverLocation <Location
   of Web Logic Server Home
   ```

3. Create a Oracle Entitlements Server Client domain, as described in Configuring OES Client Domain in a Non-JRF Environment or Configuring OES Client Domain in a JRF Environment.

8.6.3 Configuring Security Modules

Oracle Entitlements Server Client includes the following Security Modules:

- Configuring WebLogic Server Security Module
- Configuring Web Service Security Module
- Configuring Web Service Security Module on Oracle WebLogic Server
- Configuring Oracle Service Bus Security Module
- Configuring IBM WebSphere Security Module
- Configuring JBoss Security Module
- Configuring the Apache Tomcat Security Module
- Configuring Java Security Module
- Configuring RMI Security Module
- Configuring Microsoft .NET Security Module
- Configuring Microsoft SharePoint Server (MOSS) Security Module

8.6.3.1 Configuring WebLogic Server Security Module

The WebLogic Security Module is a custom Java Security Module that includes both a Policy Decision Point and a Policy Enforcement Point. It can receive requests directly from the WebLogic Server without the need for explicit authorization API calls. It will only run on the WebLogic Server container.

To configure a WebLogic Server Security Module instance, you must run the `config.sh` (located in `OES_CLIENT_HOME/oessm/bin` on UNIX) or `config.cmd` (located in `OES_CLIENT_HOME\oessm\bin` on Windows) as follows:

On UNIX:

```
config.sh -onJRF -smType wls -smConfigId mySM_WLS -serverLocation MW_
HOME/wlserver_10.3/
```

On Windows:

```
config.sh -onJRF -smType wls -smConfigId mySM_WLS -serverLocation MW_
HOME\wlserver_10.3\
```

> **Note:** If you are using a non-JRF environment, do not specify the `-onJRF` parameter.

In non-controlled and controlled-pull distribution modes, when prompted, specify the Oracle Entitlements Server schema owner and password.

Table 8–7 describes the parameters you specify on the command line.

Table 8–7 Oracle WebLogic Server Security Module Parameters

Parameter	Description
`smType`	Type of security module instance you want to create. It should be `wls`.
`smConfigId`	Name of the security module instance. For example, `mySM_WLS_Controlled`.
`serverLocation`	Location of the Oracle WebLogic Server.

Note: Non-controlled mode is the default distribution mode for Oracle WebLogic Server Security Module in a JRF environment. This will not change even if you edit the distribution mode in the `smconfig.prp` file.

For Oracle WebLogic Server Security Module in a non-JRF environment, the default distribution mode is set to controlled-push mode in the `smconfig.prp` file. If you want to change the distribution mode, refer to Section 8.6.1.2, "Configuring Non-Controlled and Controlled Pull Distribution Mode".

Controlled-push mode is not supported for Oracle WebLogic Server Security Module in a JRF enabled domain.

The Configuration Wizard is displayed. You can create an Oracle Entitlements Server Client domain in a JRF environment and a non-JRF environment. Depending on the option you select complete one of the following:

- Configuring OES Client Domain in a Non-JRF Environment
- Configuring OES Client Domain in a JRF Environment

8.6.3.1.1 Configuring OES Client Domain in a Non-JRF Environment

To create the Oracle Entitlements Server Client domain without JRF, complete the following steps:

1. The Fusion Middleware Configuration Wizard appears after you invoke the Security Module configuration tool.
2. On the Welcome screen, select the **Create a new WebLogic domain** option.

   Note: If you want to extend an existing WebLogic domain, then you must follow these steps:

   1. Select the **Extend an existing WebLogic domain** option on the Welcome screen. Click **Next**.
   2. On the Select a WebLogic Domain Directory screen, select the existing domain that you want to use. Click **Next**.
   3. On the Select Extension Source screen, choose whether to extend the domain by selecting one of the listed products, or by browsing to an extension template. Click **Next**. The Specify Domain Name and Location screen appears. Continue with step 4.

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

   Select the **Oracle Entitlements Server WebLogic Security Module - 11.1.1.0 [oesclient]** option. Click **Next**.

   Note: Ensure that you do not select the domain template **Oracle Entitlements Server for Admin Server - 11.1.1.0 [IAM_HOME]** which is associated with the Oracle Entitlements Server Administration Server.

The Specify Domain Name and Location screen appears.

4. Enter a name and a location for the domain to be created, and click **Next**.

   The Configure Administrator User Name and Password screen appears.

5. Enter a user name and a password for the administrator. The default user name is `weblogic`. Click **Next**.

   The Configure Server Start Mode and JDK screen appears.

   Note: When you enter the user name and the password for the administrator, be sure to remember them.

6. Choose a JDK from the **Available JDKs** and then select a **WebLogic Domain Startup Mode**. Click **Next**.

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

   The Select Optional Configuration screen is displayed.

7. On the Select Optional Configuration screen, you can configure **Administration Server** and **Managed Servers, Clusters, and Machines, Deployments and Services**, and **RDBMS Security Store** options. Click **Next**.

8. Optional: Configure the following Administration Server parameters:

   - Name: Valid server names are a string of characters (alphabetic and numeric). The name must be unique in the domain. For example, `AdminServer`.
   - Listen address: From the drop-down list, select a value for the listen address. See Specifying the Listen Address for information about the available values.
   - Listen port—Enter a valid value for the listen port to be used for regular, nonsecure requests (through protocols such as HTTP and T3). The default value is the next available listen port. If you leave this field blank, the default value is used. For example, `7001`.

     Note: Ensure that the value for the listen port is different from the listen port of the other Oracle Identity and Access Management components. For more information, see "Managing Ports" in the *Oracle Fusion Middleware Administrator's Guide*.

   - SSL enabled—Select this check box to enable the SSL listen port. By default, SSL is disabled for all new servers.
   - SSL listen port—Enter a valid value to be used for secure requests (through protocols such as HTTPS and T3S). The default value is the next available listen port. If you leave this field blank, the default value is used. For example, `7002`.

> **Note:** After you specify the SSL listen port value, you must update the `oracle.security.jps.pd.clientPort` property in the `smconfig.wls.controlled.prp` file or `smconfig.prp` file with the SSL listen port value. You must then run the `smconfig` tool for Oracle WebLogic Server Security Module and set the Administration Server SSL port to the port specified in `oracle.security.jps.pd.clientPort`.

9. Optional: Configure Managed Servers, as required.

   In the Configure Managed Servers screen, click **Add** and create two Managed Servers. Enter the following information:

   - Name: Enter `OES_ManagedServer_1` and `OES_ManagedServer_2`.
   - Listen address: From the drop-down list, select a value for the listen address for `OES_ManagedServer_1` and `OES_ManagedServer_2`.
   - Listen port—Enter a valid value for the listen port to be used for `OES_ManagedServer_1` and `OES_ManagedServer_2`. The default value is the next available listen port. If you leave this field blank, the default value is used. The valid listen port range is 1 to 65535.
   - SSL enabled—Select this check box to enable the SSL listen port. By default, SSL is disabled for all new servers.
   - SSL listen port—Enter a valid value to be used for secure requests (through protocols such as HTTPS and T3S) for `OES_ManagedServer_1` and `OES_ManagedServer_2`. The default value is the next available listen port. If you leave this field blank, the default value is used. The valid listen port range is 1 to 65535.

10. Optional: Configure Clusters, as required.

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

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

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

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

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

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

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

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

17. On successful domain creation you may review the folder structure and files of the WebLogic Server Security Module instance. The `jps-config.xml` configuration

file for the WebLogic Server Security Module instance configuration is located in `$DOMAIN_HOME/config/oeswlssmconfig/AdminServer`.

Setting Up Connection to an Oracle Database

After configuring OES Client domain in a non-controlled or controlled-pull distribution mode, you must set up a connection to an Oracle Database, as described in "Setting Up Connection to an Oracle Database for Security Modules Configured in a Non-JRF Environment".

8.6.3.1.2 Configuring OES Client Domain in a JRF Environment

To create the OES Client domain with JRF, complete the following steps:

1. The Fusion Middleware Configuration Wizard appears after you invoke the Security Module configuration tool.
2. On the Welcome screen, select the **Create a new WebLogic domain** option.

   Note: If you want to extend an existing WebLogic domain, then you must follow these steps:

   1. Select the **Extend an existing WebLogic domain** option on the Welcome screen. Click **Next**.
   2. On the Select a WebLogic Domain Directory screen, select the existing domain that you want to use. Click **Next**.
   3. On the Select Extension Source screen, choose whether to extend the domain by selecting one of the listed products, or by browsing to an extension template. Click **Next**. The Specify Domain Name and Location screen appears. Continue with step 4.

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

   Select the **Oracle Entitlements Server WebLogic Security Module On JRF - 11.1.1.0 [oesclient]** option. Click **Next**.

   Note: Ensure that you do not select the domain template **Oracle Entitlements Server for Admin Server - 11.1.1.0 [IAM_HOME]** which is associated with the Oracle Entitlements Server Administration Server.

   The Specify Domain Name and Location screen appears.
4. Enter a name and a location for the domain to be created, and click **Next**.

   The Configure Administrator User Name and Password screen appears.
5. Enter a user name and a password for the administrator. The default user name is `weblogic`. Click **Next**.

   The Configure Server Start Mode and JDK screen appears.

   Note: When you enter the user name and the password for the administrator, be sure to remember them.

6. Choose a JDK from the **Available JDKs** and then select a **WebLogic Domain Startup Mode**. Click **Next**.

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

   The Select Optional Configuration screen is displayed.

7. On the Select Optional Configuration screen, you can configure **Administration Server** and **Managed Servers, Clusters, and Machines, Deployments and Services**, and **RDBMS Security Store** options. Click **Next**.

8. Optional: Configure the following Administration Server parameters:

   - Name: Valid server names are a string of characters (alphabetic and numeric). The name must be unique in the domain. For example, `AdminServer`.
   - Listen address: From the drop-down list, select a value for the listen address. See Specifying the Listen Address for information about the available values.
   - Listen port—Enter a valid value for the listen port to be used for regular, nonsecure requests (through protocols such as HTTP and T3). The default value is the next available listen port. If you leave this field blank, the default value is used. For example, `7001`.

     Note: Ensure that the value for the listen port is different from the listen port of the other Oracle Identity and Access Management components. For more information, see "Managing Ports" in the *Oracle Fusion Middleware Administrator's Guide*.

   - SSL enabled—Select this check box to enable the SSL listen port. By default, SSL is disabled for all new servers.
   - SSL listen port—Enter a valid value to be used for secure requests (through protocols such as HTTPS and T3S). The default value is the next available listen port. If you leave this field blank, the default value is used. For example, `7002`.

     Note: After you specify the SSL listen port value, you must update the `oracle.security.jps.pd.clientPort` property in the `smconfig.wls.controlled.prp` file or `smconfig.prp` file with the SSL listen port value. You must then run the `smconfig` tool for Oracle WebLogic Server Security Module and set the Administration Server SSL port to the port specified in `oracle.security.jps.pd.clientPort`.

9. Optional: Configure Managed Servers, as required.

   In the Configure Managed Servers screen, click **Add** and create two Managed Servers. Enter the following information:

   - Name: Enter `OES_ManagedServer_1` and `OES_ManagedServer_2`.
   - Listen address: From the drop-down list, select a value for the listen address for `OES_ManagedServer_1` and `OES_ManagedServer_2`.

- Listen port—Enter a valid value for the listen port to be used for `OES_ManagedServer_1` and `OES_ManagedServer_2`. The default value is the next available listen port. If you leave this field blank, the default value is used. The valid listen port range is 1 to 65535.
- SSL enabled—Select this check box to enable the SSL listen port. By default, SSL is disabled for all new servers.
- SSL listen port—Enter a valid value to be used for secure requests (through protocols such as HTTPS and T3S) for `OES_ManagedServer_1` and `OES_ManagedServer_2`. The default value is the next available listen port. If you leave this field blank, the default value is used. The valid listen port range is 1 to 65535.

10. Optional: Configure Clusters, as required.

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

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

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

13. Optional: Assign the Administration Server to a machine.
14. Optional: Select Deployments, such as applications and libraries, and Services to target them to a particular cluster or server.
15. Optional: Configure RDBMS Security Store, as required.
16. On the Configuration Summary screen, review the domain configuration, and click **Create** to start creating the domain.

Setting Up Connection to an Oracle Database

After configuring OES Client domain in a non-controlled or controlled-pull distribution mode, you must set up a connection to an Oracle Database, as described in "Setting Up Connection to an Oracle Database for Security Modules Configured in a JRF Environment".

8.6.3.2 Configuring Web Service Security Module

To create a Web Service Security Module instance, you must run the `config.sh` (located in `OES_CLIENT_HOME/oessm/bin` for UNIX) or `config.cmd` (located in `OES_CLIENT_HOME\oessm\bin` for Windows) as follows:

```
config.sh -smType ws -smConfigId mySM_Ws -serverPort 9410
```

In controlled push mode, when prompted, specify the Oracle Entitlements Server Administration Server user name, Oracle Entitlements Server Administration Server password, and a new key store password for enrollment.

In non-controlled and controlled-pull distribution modes when prompted, specify the Oracle Entitlements Server schema user name and password.

Table 8–8 describes the parameters you specify on the command line.

Table 8–8 Web Service Security Module Parameter

Parameters	Description
`smType`	Type of security module instance you want to create. For Web Service security module, the value for this parameter should be `ws`.
`smConfigId`	Name of the security module instance. For example, `mySM_ws`.
`serverPort`	The web service listening port. For example, `9410`.

Note: For Web Service Security Module, the default distribution mode is set to controlled-push mode in the `smconfig.prp` file. If you want to change the distribution mode, refer to Section 8.6.1.2, "Configuring Non-Controlled and Controlled Pull Distribution Mode".

This command also creates client configuration for Webservice Security Module Instance.

8.6.3.3 Configuring Web Service Security Module on Oracle WebLogic Server

To create a Web Service Security Module instance on Oracle WebLogic Server, you must run the `config.sh` (located in `OES_CLIENT_HOME/oessm/bin` for UNIX) or `config.cmd` (located in `OES_CLIENT_HOME\oessm\bin` for Windows) as follows:

```
config.sh -onJRF -smType ws -onWLS -smConfigId mySM_WsOnWLS -serverLocation
<WebLogic_server_Home> -serverPort <WebLogic_server_port> -pdServer <oes_server_
address> -pdPort <oes_server_ssl_port> -serverUserName <username> -serverPassword
<password>
```

Note: If you are using a non-JRF environment, do not specify the `-onJRF` parameter.

In controlled push mode, when prompted, specify the Oracle Entitlements Server Administration Server user name, Oracle Entitlements Server Administration Server password, and a new key store password for enrollment.

In non-controlled and controlled-pull distribution modes when prompted, specify the Oracle Entitlements Server schema user name and password.

Table 8–9 describes the parameters you specify on the command line.

Table 8–9 Parameters for Web Service Security Module on Oracle WebLogic Server

Parameters	Description
`smType`	Type of security module instance you want to create. For Web Service security module, the value for this parameter should be `ws`.
`smConfigId`	Name of the security module instance. For example, `mySM_ws_Controlled`.
`pdServer`	The address of the Oracle Entitlements Server Administration Server.

Table 8–9 (Cont.) Parameters for Web Service Security Module on Oracle WebLogic

Parameters	Description
`pdPort`	The SSL port of the Oracle Entitlements Server Administration Server. For example, 7002.
`serverLocation`	Location of the Oracle WebLogic Server.
`serverPort`	The value for `serverPort` should be the listening port of the Web Services Security Module. For Web Service Security Module on Oracle WebLogic Server, the listening port is the Weblogic Administration Server port. Hence, for serverPort, you must specify the value of the Oracle WebLogic Administration Server port. For example, 7001.
`serverUserName`	Specify the Oracle WebLogic Server Administration username. For example: `weblogic`
`serverPassword`	Specify the Oracle WebLogic Server Administration password.

Note: For Web Service Security Module on Oracle WebLogic Server in a non-JRF environment, the default distribution mode is set to controlled-push mode in the `smconfig.prp` file. If you want to change the distribution mode, refer to Section 8.6.1.2, "Configuring Non-Controlled and Controlled Pull Distribution Mode".

Non-controlled distribution is the default distribution mode for Web Service Security Module on Oracle WebLogic Server in a JRF environment. This will not change even if you edit the distribution mode in the `smconfig.prp` file.

This command also creates client configuration for Webservice Security Module Instance on Oracle WebLogic Server.

The Configuration Wizard is displayed. You can create an OES Client domain with Web Service on Oracle WebLogic Server in a JRF environment and Web Service on Oracle WebLogic Server in a non-JRF environment. Depending on the option you select complete one of the following:

- Configuring Web Service on Oracle WebLogic Server Domain in a Non-JRF Environment
- Configuring Web Service on Oracle WebLogic Server Domain in a JRF Environment

8.6.3.3.1 Configuring Web Service on Oracle WebLogic Server Domain in a Non-JRF Environment

To create a Web Service on Oracle WebLogic Server domain in a Non-JRF environment, complete the following steps:

1. The Fusion Middleware Configuration Wizard appears after you invoke the Security Module configuration tool.
2. On the Welcome screen, select the **Create a new WebLogic domain** option.

Note: If you want to extend an existing WebLogic domain, then you must follow these steps:

1. Select the **Extend an existing WebLogic domain** option on the Welcome screen. Click **Next**.
2. On the Select a WebLogic Domain Directory screen, select the existing domain that you want to use. Click **Next**.
3. On the Select Extension Source screen, choose whether to extend the domain by selecting one of the listed products, or by browsing to an extension template. Click **Next**. The Specify Domain Name and Location screen appears. Continue with step 4.

Click **Next**. The Select Domain Source screen appears.

3. On the Select Domain Source screen, ensure that the **Generate a domain configured automatically to support the following products:** option is selected.

   Select the **Oracle Entitlements Server Web Service Security Module on Weblogic- 11.1.1.0 [oesclient]** option. Click **Next**.

   Note: Ensure that you do not select the domain template **Oracle Entitlements Server for Admin Server - 11.1.1.0 [IAM_HOME]** which is associated with the Oracle Entitlements Server Administration Server.

   The Specify Domain Name and Location screen appears.

4. Enter a name and a location for the domain to be created, and click **Next**.

   The Configure Administrator User Name and Password screen appears.

5. Enter a user name and a password for the administrator. The default user name is `weblogic`. Click **Next**.

   The Configure Server Start Mode and JDK screen appears.

   Note: When you enter the user name and the password for the administrator, be sure to remember them.

   ---

6. Choose a JDK from the **Available JDKs** and then select a **WebLogic Domain Startup Mode**. Click **Next**.

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

   The Select Optional Configuration screen is displayed.

7. On the Select Optional Configuration screen, you can configure **Administration Server** and **Managed Servers, Clusters, and Machines, Deployments and Services**, and **RDBMS Security Store** options. Click **Next**.
8. Optional: Configure the following Administration Server parameters:

   - Name: Valid server names are a string of characters (alphabetic and numeric). The name must be unique in the domain. For example, `AdminServer`.

- Listen address: From the drop-down list, select a value for the listen address. See Specifying the Listen Address for information about the available values.
- Listen port—Enter a valid value for the listen port to be used for regular, nonsecure requests (through protocols such as HTTP and T3). The default value is the next available listen port. If you leave this field blank, the default value is used. For example, `7001`.

  Note: Ensure that the value for the listen port is different from the listen port of the other Oracle Identity and Access Management components. For more information, see "Managing Ports" in the *Oracle Fusion Middleware Administrator's Guide*.

- SSL enabled—Select this check box to enable the SSL listen port. By default, SSL is disabled for all new servers.
- SSL listen port—Enter a valid value to be used for secure requests (through protocols such as HTTPS and T3S). The default value is the next available listen port. If you leave this field blank, the default value is used. For example, `7002`.

  Note: After you specify the SSL listen port value, you must update the `oracle.security.jps.pd.clientPort` property in the `smconfig.wls.controlled.prp` file or `smconfig.prp` file with the SSL listen port value. You must then run the `smconfig` tool for Oracle WebLogic Server Security Module and set the Administration Server SSL port to the port specified in `oracle.security.jps.pd.clientPort`.

9. Optional: Configure Managed Servers, as required.

   In the Configure Managed Servers screen, click **Add** and create two Managed Servers. Enter the following information:

   - Name: Enter `OES_ManagedServer_1` and `OES_ManagedServer_2`.
   - Listen address: From the drop-down list, select a value for the listen address for `OES_ManagedServer_1` and `OES_ManagedServer_2`.
   - Listen port—Enter a valid value for the listen port to be used for `OES_ManagedServer_1` and `OES_ManagedServer_2`. The default value is the next available listen port. If you leave this field blank, the default value is used. The valid listen port range is 1 to 65535.
   - SSL enabled—Select this check box to enable the SSL listen port. By default, SSL is disabled for all new servers.
   - SSL listen port—Enter a valid value to be used for secure requests (through protocols such as HTTPS and T3S) for `OES_ManagedServer_1` and `OES_ManagedServer_2`. The default value is the next available listen port. If you leave this field blank, the default value is used. The valid listen port range is 1 to 65535.

10. Optional: Configure Clusters, as required.

    For more information about configuring clusters for Oracle Identity and Access Management products, see the "Configuring High Availability for Oracle Identity

and Access Management Components" topic in the *Oracle Fusion Middleware High Availability Guide*.

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

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

13. Optional: Assign the Administration Server to a machine.
14. Optional: Select Deployments, such as applications and libraries, and Services to target them to a particular cluster or server.
15. Optional: Configure RDBMS Security Store, as required.
16. On the Configuration Summary screen, review the domain configuration, and click **Create** to start creating the domain.
17. On successful domain creation you may review the folder structure and files of the Web Service Security Module instance on Oracle WebLogic Server. The `jps-config.xml` configuration file for the Web Service Security Module instance on Oracle WebLogic Server is located in `$DOMAIN_HOME/config/oeswlssmconfig/AdminServer`.

Setting Up Connection to Oracle Database

After configuring Web Service on Oracle WebLogic Server domain in a non-controlled or controlled-pull distribution mode, you must set up a connection to an Oracle Database, as described in "Setting Up Connection to an Oracle Database for Security Modules Configured in a Non-JRF Environment".

8.6.3.3.2 Configuring Web Service on Oracle WebLogic Server Domain in a JRF Environment

To create the Web Service on Oracle WebLogic Server domain in a JRF environment, complete the following steps:

1. The Fusion Middleware Configuration Wizard appears after you invoke the Security Module configuration tool.
2. On the Welcome screen, select the **Create a new WebLogic domain** option.

   Note: If you want to extend an existing WebLogic domain, then you must follow these steps:

   1. Select the **Extend an existing WebLogic domain** option on the Welcome screen. Click **Next**.
   2. On the Select a WebLogic Domain Directory screen, select the existing domain that you want to use. Click **Next**.
   3. On the Select Extension Source screen, choose whether to extend the domain by selecting one of the listed products, or by browsing to an extension template. Click **Next**. The Specify Domain Name and Location screen appears. Continue with step 4.

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

Select the **Oracle Entitlements Server Web Service Security Module on Weblogic and JRF- 11.1.1.0 [oesclient]** option. Click **Next**.

> **Note:** Ensure that you do not select the domain template **Oracle Entitlements Server for Admin Server - 11.1.1.0 [IAM_HOME]** which is associated with the Oracle Entitlements Server Administration Server.

The Specify Domain Name and Location screen appears.

4. Enter a name and a location for the domain to be created, and click **Next**.

   The Configure Administrator User Name and Password screen appears.

5. Enter a user name and a password for the administrator. The default user name is `weblogic`. Click **Next**.

   The Configure Server Start Mode and JDK screen appears.

   > **Note:** When you enter the user name and the password for the administrator, be sure to remember them.

6. Choose a JDK from the **Available JDKs** and then select a **WebLogic Domain Startup Mode**. Click **Next**.

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

   The Select Optional Configuration screen is displayed.

7. On the Select Optional Configuration screen, you can configure **Administration Server** and **Managed Servers, Clusters, and Machines, Deployments and Services**, and **RDBMS Security Store** options. Click **Next**.

8. Optional: Configure the following Administration Server parameters:

   - Name: Valid server names are a string of characters (alphabetic and numeric). The name must be unique in the domain. For example, `AdminServer`.
   - Listen address: From the drop-down list, select a value for the listen address. See Specifying the Listen Address for information about the available values.
   - Listen port—Enter a valid value for the listen port to be used for regular, nonsecure requests (through protocols such as HTTP and T3). The default value is the next available listen port. If you leave this field blank, the default value is used. For example, `7001`.

     > **Note:** Ensure that the value for the listen port is different from the listen port of the other Oracle Identity and Access Management components. For more information, see "Managing Ports" in the *Oracle Fusion Middleware Administrator's Guide*.

   - SSL enabled—Select this check box to enable the SSL listen port. By default, SSL is disabled for all new servers.

- SSL listen port—Enter a valid value to be used for secure requests (through protocols such as HTTPS and T3S). The default value is the next available listen port. If you leave this field blank, the default value is used. For example, `7002`.

Note: After you specify the SSL listen port value, you must update the `oracle.security.jps.pd.clientPort` property in the `smconfig.wls.controlled.prp` file or `smconfig.prp` file with the SSL listen port value. You must then run the `smconfig` tool for Oracle WebLogic Server Security Module and set the Administration Server SSL port to the port specified in `oracle.security.jps.pd.clientPort`.

---

9. Optional: Configure Managed Servers, as required.

   In the Configure Managed Servers screen, click **Add** and create two Managed Servers. Enter the following information:

   - Name: Enter `OES_ManagedServer_1` and `OES_ManagedServer_2`.
   - Listen address: From the drop-down list, select a value for the listen address for `OES_ManagedServer_1` and `OES_ManagedServer_2`.
   - Listen port—Enter a valid value for the listen port to be used for `OES_ManagedServer_1` and `OES_ManagedServer_2`. The default value is the next available listen port. If you leave this field blank, the default value is used. The valid listen port range is 1 to 65535.
   - SSL enabled—Select this check box to enable the SSL listen port. By default, SSL is disabled for all new servers.
   - SSL listen port—Enter a valid value to be used for secure requests (through protocols such as HTTPS and T3S) for `OES_ManagedServer_1` and `OES_ManagedServer_2`. The default value is the next available listen port. If you leave this field blank, the default value is used. The valid listen port range is 1 to 65535.

10. Optional: Configure Clusters, as required.

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

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

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

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

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

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

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

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

Setting Up Connection to Oracle Database

After configuring Web Service on Oracle WebLogic Server domain in a non-controlled or controlled-pull distribution mode, you must set up a connection to an Oracle Database, as described in "Setting Up Connection to an Oracle Database for Security Modules Configured in a JRF Environment".

8.6.3.4 Configuring Oracle Service Bus Security Module

To create a Oracle Service Bus Security Module instance, you must run the `config.sh` (located in `OES_CLIENT_HOME/oessm/bin` on UNIX) or `config.cmd` (located in `OES_CLIENT_HOME\oessm\bin` on Windows) as follows:

```
config.sh -onJRF -smType wls -smConfigId myosb_WLS -serverLocation <server_
location>
```

Table 8–10 Oracle Service Bus Security Module Parameters

Parameter	Description
`smType`	Type of security module instance you want to create. For example, `jboss`.
`smConfigId`	Name of the security module instance. For example, `mySM_WLS`.
`serverLocation`	The location of Oracle WebLogic Server.

> **Note:** Non-controlled distribution is the default distribution mode for Oracle Service Bus Security Module. This will not change even if you edit the distribution mode in the `smconfig.prp` file.

The Configuration Wizard is displayed. You can create an OES Client domain with Oracle Service Bus environment as follows:

1. The Fusion Middleware Configuration Wizard appears after you invoke the Security Module configuration tool.
2. On the Welcome screen, select the **Create a new WebLogic domain** option. Click **Next**.

   The Select Domain Source screen appears.
3. On the Select Domain Source screen, ensure that the **Generate a domain configured automatically to support the following products:** option is selected.

   Select the **Oracle Entitlements Server Security Module On Service Bus - 11.1.1.0 [OESCLIENT]** option. Click **Next**.

   > **Note:** Ensure that you do not select the domain template **Oracle Entitlements Server for Admin Server - 11.1.1.0 [IAM_HOME]** which is associated with the Oracle Entitlements Server Administration Server.

   The Specify Domain Name and Location screen appears.

4. Enter a name and a location for the domain to be created, and click **Next**.

   The Configure Administrator User Name and Password screen appears.

5. Enter a user name and a password for the administrator. The default user name is `weblogic`. Click **Next**.

   The Configure Server Start Mode and JDK screen appears.

   Note: When you enter the user name and the password for the administrator, be sure to remember them.

6. Choose a JDK from the **Available JDKs** and then select a **WebLogic Domain Startup Mode**. Click **Next**.

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

   The Select Optional Configuration screen is displayed.

7. On the Select Optional Configuration screen, you can configure **Administration Server** and **Managed Servers, Clusters, and Machines, Deployments and Services**, and **RDBMS Security Store** options. Click **Next**.

8. Optional: Configure the following Administration Server parameters:

   - Name: Valid server names are a string of characters (alphabetic and numeric). The name must be unique in the domain. For example, `AdminServer`.
   - Listen address: From the drop-down list, select a value for the listen address. See Specifying the Listen Address for information about the available values.
   - Listen port—Enter a valid value for the listen port to be used for regular, nonsecure requests (through protocols such as HTTP and T3). The default value is the next available listen port. If you leave this field blank, the default value is used. For example, `7001`.

     Note: Ensure that the value for the listen port is different from the listen port of the other Oracle Identity and Access Management components. For more information, see "Managing Ports" in the *Oracle Fusion Middleware Administrator's Guide*.

   - SSL enabled—Select this check box to enable the SSL listen port. By default, SSL is disabled for all new servers.
   - SSL listen port—Enter a valid value to be used for secure requests (through protocols such as HTTPS and T3S). The default value is the next available listen port. If you leave this field blank, the default value is used. For example, `7002`.

Note: After you specify the SSL listen port value, you must update the `oracle.security.jps.pd.clientPort` property in the `smconfig.wls.controlled.prp` file or `smconfig.prp` file with the SSL listen port value. You must then run the `smconfig` tool for Oracle WebLogic Server Security Module and set the Administration Server SSL port to the port specified in `oracle.security.jps.pd.clientPort`.

9. Optional: Configure Managed Servers, as required.

   In the Configure Managed Servers screen, click **Add** and create two Managed Servers. Enter the following information:

   - Name: Enter `OES_ManagedServer_1` and `OES_ManagedServer_2`.
   - Listen address: From the drop-down list, select a value for the listen address for `OES_ManagedServer_1` and `OES_ManagedServer_2`.
   - Listen port—Enter a valid value for the listen port to be used for `OES_ManagedServer_1` and `OES_ManagedServer_2`. The default value is the next available listen port. If you leave this field blank, the default value is used. The valid listen port range is 1 to 65535.
   - SSL enabled—Select this check box to enable the SSL listen port. By default, SSL is disabled for all new servers.
   - SSL listen port—Enter a valid value to be used for secure requests (through protocols such as HTTPS and T3S) for `OES_ManagedServer_1` and `OES_ManagedServer_2`. The default value is the next available listen port. If you leave this field blank, the default value is used. The valid listen port range is 1 to 65535.

10. Optional: Configure Clusters, as required.

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

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

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

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

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

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

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

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

Setting Up Connection to Oracle Database

After configuring Oracle Service Bus Security Module in a non-controlled or controlled-pull distribution mode, you must set up a connection to an Oracle Database, as described in "Setting Up Connection to an Oracle Database for Security Modules Configured in a JRF Environment".

Configuring Authorization Provider

You must configure an Authorization provider. For information about configuring an Authorization provider, see "Configure Authorization providers" topic in the *Oracle Fusion Middleware Oracle WebLogic Server Administration Console Online Help* document, available at the following link:

`http://docs.oracle.com/cd/E23943_01/apirefs.1111/e13952/taskhelp/security/ConfigureAuthorizationProviders.html`

Configuring Role Mapping Provider

You must configure a Role Mapping provider. For information about configuring a Role Mapping provider, see "Configure Role Mapping providers" topic in the *Oracle Fusion Middleware Oracle WebLogic Server Administration Console Online Help* document, available at the following link:

`http://docs.oracle.com/cd/E23943_01/apirefs.1111/e13952/taskhelp/security/ConfigureRoleMappingProviders.html`

8.6.3.5 Configuring IBM WebSphere Security Module

For information on configuring IBM WebSphere Security Module, refer to "Configuring IBM WebSphere Security Module" in the *Oracle Fusion Middleware Third-Party Application Server Guide for Oracle Identity and Access Management*.

8.6.3.6 Configuring JBoss Security Module

To create a JBoss Security Module instance, you must run the `config.sh` (located in `OES_CLIENT_HOME/oessm/bin` on UNIX) or `config.cmd` (located in `OES_CLIENT_HOME\oessm\bin` on Windows) as follows:

```
config.sh -smType jboss -smConfigId mySM_JBOSS -serverLocation
<middleware>/jbosslocation/
```

Table 8–11 JBoss Security Module Parameters

Parameter	Description
`smType`	Type of security module instance you want to create. For example, `jboss`.
`smConfigId`	Name of the security module instance. For example, `mySM_WLS`.
`serverLocation`	The location of JBoss Application Server.

Note: Controlled-push distribution is the default distribution mode for JBoss Security Module. If you want to change the distribution mode, refer to Section 8.6.1.2, "Configuring Non-Controlled and Controlled Pull Distribution Mode".

To make controlled-push mode work, you must login to WebLogic Administration console and go to **Environment>Servers>AdminServer>SSL**. The **Settings for AdminServer** page is displayed. Click on **Advanced** tab and select **Use Server Certs**.

8.6.3.7 Configuring the Apache Tomcat Security Module

To create a Apache Tomcat Security Module instance, you must run the `config.sh` (located in `OES_CLIENT_HOME/oessm/bin` on UNIX) or `config.cmd` (located in `OES_CLIENT_HOME\oessm\bin` on Windows) as follows:

```
config.sh -smType tomcat -smConfigId my_tomcat_sm_push pdServer <oes_server_
address> -pdPort <oes_server_port> -sslPort <oes_server_ssl_port> -serverLocation
<apache-tomcat Home> -jaxwsRIHome  <jaxwsRI_Home>  -serverUserName <username>
-serverPassword <password>
```

Table 8–12 Apache Tomcat Security Module Parameters

Parameter	Description
`smType`	Type of security module instance you want to create. For example, `tomcat`.
`smConfigId`	Name of the security module instance. For example, `my_tomcat_sm_push`.
`pdServer`	The address of the Oracle Entitlements Server Administration Server.
`pdPort`	The port number of the Oracle Entitlements Server Administration Server. For example, `7002`.
`sslPort`	The SSL port number of the Oracle Entitlements Server Administration Server. For example, `8449`.
`serverLocation`	The location of Apache Tomcat Server.
`jaxwsRIHome`	The location of JAXWS-RI **Note**: JAXWS support is required in controlled-push mode. Apache Tomcat does not have JAXWS support by default. You can download JAXWS-RI from the following location: `http://jax-ws.java.net/2.1.7/`
`serverUserName`	Specify the Oracle WebLogic Server Administration username. For example: `weblogic`
`serverPassword`	Specify the Oracle WebLogic Server Administration password.

Note: Controlled-push distribution is the default distribution mode for Apache Tomcat Security Module. If you want to change the distribution mode, refer to Section 8.6.1.2, "Configuring Non-Controlled and Controlled Pull Distribution Mode".

To make controlled-push mode work, you must login to WebLogic Administration console and go to **Environment>Servers>AdminServer>SSL**. The **Settings for AdminServer** page is displayed. Click on **Advanced** tab and select **Use Server Certs**.

8.6.3.8 Configuring Java Security Module

To create a Java Security Module instance, you must run the `config.sh` (located in `OES_CLIENT_HOME/oessm/bin` on UNIX) or `config.cmd` (located in `OES_CLIENT_HOME\oessm\bin` on Windows) as follows:

Note: If you are using Java Security Module in the proxy mode with Web Service Security Module or RMI Security Module, then you must use `oes-ws-client.jar` or `oes-rmi-client.jar` and ensure that you do not use `oes-client.jar`.

```
config.sh -smType java -smConfigId mySM_Java
```

In controlled push mode, you will be prompted for the Oracle Entitlements Server Administration Server username, password, and a new key store password for enrollment.

In non-controlled and controlled pull modes, you will be prompted for Oracle Entitlements Server schema username, and Password.

Table 8–13 describes the parameters you specify on the command line.

Table 8–13 JSE Security Module Parameters

Parameter	Description
`smType`	Type of security module instance you want to create. For example, `java`.
`smConfigId`	Name of the security module instance. For example, `mySM_java`.

Note: Controlled-push distribution is the default distribution mode for JSE Security Module. If you want to change the distribution mode, refer to Section 8.6.1.2, "Configuring Non-Controlled and Controlled Pull Distribution Mode".

The Java Security Module Instance is created at `OES_CLIENT_HOME/oes_sm_instances/mySM_java`. If you use the default values described in Table 8–13.

8.6.3.9 Configuring RMI Security Module

To configure a RMI Security Module Instance, you must run the `config.sh` (located in `OES_CLIENT_HOME/oessm/bin` for UNIX) or `config.cmd` (located in `OES_CLIENT_HOME\oessm\bin` for Windows) as follows:

```
config.sh -smType rmi -smConfigId mySM_Rmi -serverPort 9405
```

In controlled push mode, when prompted, specify the Oracle Entitlements Server Administration Server user name, Oracle Entitlements Server Administration Server password, and a new key store password for enrollment.

In non-controlled and controlled-pull distribution modes when prompter specify the Oracle Entitlements Server schema username and password.

Table 8–14 describes the parameters you specify on the command line.

Table 8–14 RMI Security Module Parameters

Parameter	Description
`smType`	The type of security module instance you want to create. For example, `rmi`.
`smConfigId`	The name of the security module instance. For example, `mySM_rmi`.
`serverPort`	The RMI listening port. For example, `9405`.

> **Note:** Controlled-push distribution is the default distribution mode for RMI Security Module. If you want to change the distribution mode, refer to Section 8.6.1.2, "Configuring Non-Controlled and Controlled Pull Distribution Mode".

This command also creates client configuration for the RMI Security Module Instance.

8.6.3.10 Configuring Microsoft .NET Security Module

This section includes the following topics:

- Prerequisites for Configuring .NET Security Module
- Microsoft .NET Configuration Scenarios

8.6.3.10.1 Prerequisites for Configuring .NET Security Module

Before configuring .NET Security Module, you must complete the following steps:

Open the `dotnetsm_config.properties` file (located in `<MW_Home>\as_1\oessm\dotnetsm\configtool`) and update the following information:

- **application.config.file**: Specify the path of the configuration file based on the type of .Net application. For example: `app.config` or `web.config`
- **application.log4NetXmlfile**: Specify the location of `log4net.xml` configuration file. If you do not have an existing logging configuration file specify the default location (`OES_CLIENT_HOME/oessm/dotnetsm/logging/log4Net.xml`).
- **wssm.smurl**: Specify the OES webservice uri exposed through the WSSM in the following format:

  `http://<host>:<port>/Ssmws`

- **gac.utility**: Specify the Microsoft .NET Framework Global Assembly Cache Utility Location. You can define the following operations:

  `config`: If you select this option, then SMconfig tool registers `OES-PEP.dll` and `log4NET.dll` in GAC Utility.

  `remove`: If you select this option, then SMconfig tool removes the DLL from the GAC util and removes the configuration parameters from `application.config.file`.

8.6.3.10.2 Microsoft .NET Configuration Scenarios

You can configure .NET Security Module in the following scenarios:

- Scenario 1: .NET and Web Service on a Single Machine
- Scenario 2: .NET and Web Service on Different Machines

Scenario 1: .NET and Web Service on a Single Machine

If .NET and Web Service are installed on a single machine, the following configurations are possible:

- Configuring .NET Security Module and Web Service Security Module
- Configuring .NET Security Module

Configuring .NET Security Module and Web Service Security Module

Perform the configuration in this scenario if .NET and Web Service are installed on a single machine, and you want to configure .NET Security Module and Web Service Security Module.

Run the `config.cmd` located in `OES_CLIENT_HOME\oessm\bin` directory (on Windows), as follows:

```
config.cmd -smType dotnetws -prpFileName <ws_config> -dotnetprpFileName <dotnetsm_
config> -smConfigId myDotnet -pdServer <oes_server_address> -pdPort <oes_server_
ssl_port> -WSListeningPort 9410
```

Table 8–15 describes the parameters you specify on the command line.

Table 8–15 .NET Security Module Parameters

Parameter	Description
`smType`	The type of security module instance you want to create. For example, `dotnetws`.
`smConfigId`	The name of the security module instance. For example, `myDotnet`.
`prpFileName`	Specify the path to the `smconfig.prp` file located in `<OES_Client_Home>\oessm\wssm\configtool`.
`dotnetprpFileName`	Specify the path to the `dotnetsm_config.properties` file located in `<OES_Client_Home>\oessm\dotnetsm\configtool`.
`pdServer`	The address of the Oracle Entitlements Server Administration Server.
`pdPort`	The port number of the Oracle Entitlements Server Administration Server. For example, `7002`.
`WSListeningPort`	The web service listening port. For example, `9410`.

This command also creates client configuration for the .NET Security Module Instance.

Configuring .NET Security Module

Perform the configuration in this scenario if .NET and Web Service are installed on a single machine, and Web Service Security Module is already configured.

Before you configure a .NET Security Module instance using the command mentioned below, ensure that you have configured the Web Service Security Module, as described in Configuring Web Service Security Module on Oracle WebLogic Server.

Run the `config.cmd` (located in `OES_CLIENT_HOME\oessm\bin`) for Windows as follows:

```
config.cmd -smType dotnet -smConfigId myDotnet -prpFileName <ws_config>
-dotnetprpFileName <dotnetsm_config>
```

Table 8–17 describes the parameters you specify on the command line.

Table 8–16 .NET Security Module Parameters

Parameter	Description
`smType`	The type of security module instance you want to create. For example, `dotnet`.
`smConfigId`	The name of the security module instance. For example, `myDotnet`.
`prpFileName`	Specify the path to the `smconfig.prp` file located in `<OES_Client_Home>\oessm\wssm\configtool`.
`dotnetprpFileName`	Specify the path to the `dotnetsm_config.properties` file located in `<OES_Client_Home>\oessm\dotnetsm\configtool`.

This command also creates client configuration for the .NET Security Module Instance.

Ensure that the `application.config` file for your .NET application contains the `SsmUrl`, `SsmId` and `log4NetXml` values in the `appSettings` section.

For example:

```
<appSettings>
    <add key="SsmUrl" value="<wssm.smurl>"
    <add key="SsmId" value="<smConfigId>"/>
    <add key="FailureRetryCount" value="3"/>
    <add key="FailbackTimeoutMilliSecs" value="180000"/>
    <add key="RequestTimeoutMilliSecs" value="10000"/>
    <add key="SynchronizationIntervalMilliSecs" value="60000"/>
    <add key="log4NetXmlfile" value="<application.log4NetXmlfile> "/>
  </appSettings>
```

Scenario 2: .NET and Web Service on Different Machines

Perform the configuration in this scenario if .NET and Web Service are installed on different machines.

Before you configure a .NET Security Module instance using the command mentioned below, ensure that you have configured the Web Service Security Module, as described in Configuring Web Service Security Module on Oracle WebLogic Server.

Run the `config.cmd` (located in `OES_CLIENT_HOME\oessm\bin`) for Windows as follows:

```
config.cmd -smType dotnet -smConfigId myDotnet -prpFileName <ws_config>
-dotnetprpFileName <dotnetsm_config>
```

Table 8–17 describes the parameters you specify on the command line.

Table 8–17 .NET Security Module Parameters

Parameter	Description
`smType`	The type of security module instance you want to create. For example, `dotnet`.
`smConfigId`	The name of the security module instance. For example, `myDotnet`.
`prpFileName`	Specify the path to the `smconfig.prp` file located in `<OES_Client_Home>\oessm\wssm\configtool`.
`dotnetprpFileName`	Specify the path to the `dotnetsm_config.properties` file located in `<OES_Client_Home>\oessm\dotnetsm\configtool`.

This command also creates client configuration for the .NET Security Module Instance.

Ensure that the `application.config` file for your .NET application contains the `SsmUrl`, `SsmId` and `log4NetXml` values in the `appSettings` section.

For example:

```
<appSettings>
    <add key="SsmUrl" value="<wssm.smurl>"
    <add key="SsmId" value="<smConfigId>"/>
    <add key="FailureRetryCount" value="3"/>
    <add key="FailbackTimeoutMilliSecs" value="180000"/>
    <add key="RequestTimeoutMilliSecs" value="10000"/>
    <add key="SynchronizationIntervalMilliSecs" value="60000"/>
    <add key="log4NetXmlfile" value="<application.log4NetXmlfile> "/>
  </appSettings>
```

8.6.3.11 Configuring Microsoft SharePoint Server (MOSS) Security Module

This section includes the following topics:

- Prerequisites for Configuring MOSS Security Module
- MOSS Configuration Scenarios
- Running Resource Discovery Tool
- Migrating Resource Policies

8.6.3.11.1 Prerequisites for Configuring MOSS Security Module

Before configuring a MOSS Security Module instance, you must ensure the following:

- Microsoft SharePoint Server (MOSS) is installed on your machine.
- The MOSS Web Application, associated with site collections and other resources to be protected by OES MOSS Security Module has been created.

8.6.3.11.2 MOSS Configuration Scenarios

You can configure MOSS Security Module in the following scenarios:

- Scenario 1: MOSS and Web Service on a Single Machine

- Scenario 2: MOSS and Web Service on Different Machines

Scenario 1: MOSS and Web Service on a Single Machine

If MOSS and Web Service are installed on a single machine, the following configurations are possible:

- Configuring MOSS Security Module and Web Service Security Module
- Configuring MOSS Security Module

Configuring MOSS Security Module and Web Service Security Module

Perform the configuration in this scenario if MOSS and Web Service are installed on a single machine, and you want to configure MOSS Security Module and Web Service Security Module.

Run the `config.cmd` file located in `OES_CLIENT_HOME\oessm\bin` directory (on Windows), as follows:

```
config.cmd -smType mossws -prpFileName <ws_config> -mossprpFileName <moss_config>
-smConfigId myMoss -pdServer <oes_server_address> -pdPort <oes_server_ssl_port>
-WSListeningPort 9410
```

Table 8–18 describes the parameters you specify on the command line.

Table 8–18 MOSS Security Module Parameters

Parameter	Description
`smType`	The type of security module instance you want to create. For example, `mossws`.
`smConfigId`	The name of the security module instance. For example, `myMoss`.
`prpFileName`	Specify the path to the `smconfig.prp` file located in `<OES_Client_Home>\oessm\wssm\configtool`.
`mossprpFileName`	Specify the path to the `moss_config.properties` file located in `<OES_Client_Home>\oessm\mosssm\adm\configtool`.
`pdServer`	The address of the Oracle Entitlements Server Administration Server.
`pdPort`	The port number of the Oracle Entitlements Server Administration Server. For example, `7002`.
`WSListeningPort`	The web service listening port. For example, `9410`.

This command also creates client configuration for the MOSS Security Module Instance.

Configuring MOSS Security Module

Perform the configuration in this scenario if MOSS and Web Service are installed on a single machine, and Web Service Security Module is already configured.

Before you configure a MOSS Security Module instance using the command mentioned below, ensure that you have configured the Web Service Security Module, as described in Configuring Web Service Security Module on Oracle WebLogic Server.

Run the `config.cmd` file located in `OES_CLIENT_HOME\oessm\bin` directory (on Windows), as follows:

```
config.cmd -smType moss -smConfigId myMoss -prpFileName <ws_config>
```

```
-mossprpFileName <moss_config>
```

Table 8–20 describes the parameters you specify on the command line.

Table 8–19 MOSS Security Module Parameters

Parameter	Description
`smType`	The type of security module instance you want to create. For example, `moss`.
`smConfigId`	The name of the security module instance. For example, `myMoss`.
`prpFileName`	Specify the path to the `smconfig.prp` file located in `<OES_Client_Home>\oessm\wssm\configtool`.
`mossprpFileName`	Specify the path to the `moss_config.properties` file located in `<OES_Client_Home>\oessm\mosssm\adm\configtool`.

This command also creates client configuration for the MOSS Security Module Instance.

Scenario 2: MOSS and Web Service on Different Machines

Perform the configuration in this scenario if MOSS and Web Service are installed on different machines.

Before you configure a MOSS Security Module instance using the command mentioned below, ensure that you have configured the Web Service Security Module, as described in Configuring Web Service Security Module on Oracle WebLogic Server.

Run the `config.cmd` file located in `OES_CLIENT_HOME\oessm\bin` directory (on Windows), as follows:

```
config.cmd -smType moss -smConfigId myMoss -prpFileName <ws_config>
-mossprpFileName <moss_config>
```

Table 8–20 describes the parameters you specify on the command line.

Table 8–20 MOSS Security Module Parameters

Parameter	Description
`smType`	The type of security module instance you want to create. For example, `moss`.
`smConfigId`	The name of the security module instance. For example, `myMoss`.
`prpFileName`	Specify the path to the `smconfig.prp` file located in `<OES_Client_Home>\oessm\wssm\configtool`.
`mossprpFileName`	Specify the path to the `moss_config.properties` file located in `<OES_Client_Home>\oessm\mosssm\adm\configtool`.

This command also creates client configuration for the MOSS Security Module Instance.

8.6.3.11.3 Running Resource Discovery Tool

You must run the Resource Discovery tool to locate the MOSS resources.

Run the `MOSSResourceDiscovery.exe` file, located in `<OES_CLIENT_HOME/oessm/mosssm/lib` directory (on Windows). You will be prompted for the following parameters:

- **Enter the folder path where you want to create OES policy file** - Specify the path of the folder where the resource files will be created. Note that the directory used for storing the exported resources must be created beforehand.
- **Enter Path where Admin Url file is located** - Specify the path to `<OES_CLIENT_HOME/oessm/mosssm/adm/discovery/AdmUrls.txt` file. This file is used to extract the admin URLs.
- **Enter SharePoint site URL and DONOT append url with /. e.g. http://sharepoint01** - Specify the URL of the top level MOSS sites to be protected by OES.
- **Enter Application Name of the MOSS application to be protected by OES e.g. MossApp -** Specify the name of the MOSS application to be protected by OES.

> **Note:** Ensure that the MOSS application name that you provide is same as the value defined for `moss.app.name` parameter in `moss_config.properties` file.

- **Enter Resource Type of all the MOSS resources e.g. MossResourceType -** Specify the resource type of all the MOSS resources to be protected by OES.

> **Note:** Ensure that the MOSS resource type that you provide is same as the value defined for `moss.resource.type` parameter in `moss_config.properties` file.

Following is a sample execution of `MOSSResourceDiscovery.exe` file:

```
C:\Oracle\Middleware\Oracle_OESClient\oessm\mosssm\lib>MOSSResourceDiscovery.exe
-----------------------------------------------------------
         Welcome to the MOSS Resource Discovery
-----------------------------------------------------------
Enter the folder path where you want to create OES policy file

c:\inetpub\wwwroot\wss\VirtualDirectories\9581\policy

Enter Path where Admin Url file is located

C:\Oracle\Middleware\Oracle_OESClient\oessm\mosssm\adm\Discovery\AdmUrls.txt

Enter SharePoint site URL and DONOT append url with /. e.g. http://sharepoint01

http://alesw2k8:9581

Enter Application Name of the MOSS application to be protected by OES e.g. MossApp

MossApp

Enter Resource Type of all the MOSS resources e.g. MossResourceType

MossResourceType

Resource Discovery starts....
```

```
SpSitePath is http://alesw2k8:9581
```

8.6.3.11.4 Migrating Resource Policies

To migrate the MOSS resource policies to OES policy store, complete the following steps:

1. Go to `OES_CLIENT_HOME/oessm/bin` directory (on Windows), or `OES_CLIENT_HOME\oessm\bin` directory (on UNIX)
2. Run the `manage-policy.cmd` file (on Windows), or `manage-policy.sh` file (on UNIX)

Following is a sample execution of `manage-policy.cmd` file:

```
C:\Oracle\Middleware\Oracle_OESClient\oessm\bin>manage-policy.cmd

Please input the application name for the protected MOSS application e.g MossApp:
MossApp

Input the resource type for the MOSS resources e.g MossResourceType:
MossResourceType

Input the Moss resource file:
c:\inetpub\wwwroot\wss\VirtualDirectories\9581\policy\object

Creating resource: /_layouts
```

8.6.4 Locating Security Module Instances

The Oracle Entitlements Server security module instances are created in the `OES_CLIENT_HOME/oes_sm_instances`. directory.

For Oracle WebLogic Server security module, the domain configuration is located in `DOMAIN_HOME/config/fmwconfig`.

You can create, delete, or modify the security module instances, as required.

8.6.5 Using the Java Security Module

After configuring Java Security Module for your program, you must start the Java Security module for your program by completing the following:

1. Set a new Java System Property `-Doracle.security.jps.config` and specify the location of the `jps-config.xml` file (located in `OES_CLIENT_HOME/oes_sm_instances/<SM_NAME>/config`) as the value.
2. Enter `oes-client.jar` (located in `OES_CLIENT_HOME/modules/oracle.oes_sm.1.1.1`) into the classpath of the program.

When a Security Module is configured as a proxy client, set the `authentic.identity.cache.enabled` system property to true. The configuration is based on the type of Security Module being used and is done for the JVM in which the Web Services or RMI Security Module remote proxy is executing.

Specifically:

- If the Security Module is a WebLogic Server Security Module, the system property `-Dauthentic.identity.cache.enabled=true` should be appended to the JAVA_OPTIONS environment variable in the setDomainEnv.sh script on Unix or the setDomainEnv.cmd script on Windows.

- If the Security Module is a Java Security Module, the system property `-Dauthentic.identity.cache.enabled=true` should be added to the program being protected by the Java Security Module.

8.6.6 Configuring the PDP Proxy Client

You can configure a PDP Proxy Client for your web service Security Module or RMI Security Module, as described in Table 8–21:

Table 8–21 PDP Proxy Client Security Module Parameters

Parameter	Description
`oracle.security.jps.pdp.isProxy`	Specify `true` as the value.
`oracle.security.jps.pdp.PDPTransport`	Specify Web Service (`WS`) or (RMI).
`oracle.security.jps.pdp.proxy.PDPAddress`	Specify `http://hostname:port` (WS) or `rmi://hostname:port` (RMI).

You must run the `config.sh` (located in `OES_CLIENT_HOME/oessm/bin` on UNIX) or `config.cmd` (located in `OES_CLIENT_HOME\oessm\bin` on Windows) as shown in the following example:

For Java Security Module:

```
OES_CLIENT_HOME/oessm/bin/config.sh -smType <SM_TYPE> -smConfigId <SM_NAME>
```

The `SM_TYPE` can be `java`, `wls`, or `was`. and for `SM_NAME` enter an appropriate name.

Note: For a sample procedure of configuring the PDP Proxy client, refer to Appendix I, "Configuring the PDP Proxy Client for Web Service Security Module".

8.7 Getting Started with Oracle Entitlements Server After Installation

After installing Oracle Entitlements Server, refer to the following documents:

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

9

Configuring Oracle Privileged Account Manager

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

- Overview
- Important Note Before You Begin
- Installation and Configuration Roadmap for Oracle Privileged Account Manager
- Optional: Enabling TDE in Oracle Privileged Account Manager Data Store
- Configuring Oracle Privileged Account Manager and Oracle Identity Navigator in a New WebLogic Domain
- Starting the Oracle WebLogic Administration Server
- Post-Installation Tasks
- Starting the Managed Server
- Assigning the Application Configurator Role to a User
- Optional: Setting Up Non-TDE Mode
- Optional: Configuring OPAM Console
- Verifying Oracle Privileged Account Manager
- Getting Started with Oracle Privileged Account Manager After Installation

9.1 Overview

For an introduction to the Oracle Privileged Account Manager, see "Understanding Oracle Privileged Account Manager" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Privileged Account Manager*.

9.2 Important Note Before You Begin

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

9.3 Installation and Configuration Roadmap for Oracle Privileged Account Manager

Table 9–1 lists the tasks for installing and configuring Oracle Privileged Account Manager.

Table 9–1 Installation and Configuration Flow for Oracle Privileged Account Manager

No.	Task	Description
1	Review installation concepts in the Installation Planning Guide.	Read the *Oracle Fusion Middleware Installation Planning Guide*, which describes the process for various users to install or upgrade to Oracle Fusion Middleware 11*g* (11.1.2) depending on the user's existing environment.
2	Review the system requirements and certification documents to ensure that your environment meets the minimum installation requirements for the components you are installing.	For more information, see Section 2.1, "Reviewing System Requirements and Certification".
3	Obtain the Oracle Fusion Middleware Software.	For more information, see Section 3.2.1, "Obtaining the Oracle Fusion Middleware Software"
4	Review the Database requirements.	For more information, see Section 3.2.2, "Database Requirements".
5	Run Oracle Fusion Middleware Repository Creation Utility (RCU) to create and load the appropriate schemas for Oracle Identity and Access Management products.	For more information, see Section 3.2.3, "Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU)". **Note:** Oracle Privileged Account Manager schema must be created by a Database user with `SYSDBA` privileges.
6	Review WebLogic Server and Middleware Home requirements.	For more information, see Section 3.2.4, "WebLogic Server and Middleware Home Requirements".
7	Start the Oracle Identity and Access Management Installer.	For more information, see Section 3.2.6, "Starting the Oracle Identity and Access Management Installer".
8	Install the Oracle Identity and Access Management 11*g* software.	Oracle Privileged Account Manager is included in the Oracle Identity and Access Management Suite. You can use the Oracle Identity and Access Management 11*g* Installer to install Oracle Identity and Access Management Suite. For more information, see Section 3.2.7, "Installing Oracle Identity and Access Management 11g Release 2 (11.1.2.2.0)".
9	Optional: Enable TDE in OPAM data store.	For more information, see Section 9.4, "Optional: Enabling TDE in Oracle Privileged Account Manager Data Store"
10	Run the Oracle Fusion Middleware Configuration Wizard to configure your Oracle Identity and Access Management products in a new or existing WebLogic domain.	For more information, see Section 9.5, "Configuring Oracle Privileged Account Manager and Oracle Identity Navigator in a New WebLogic Domain".

Table 9–1 (Cont.) Installation and Configuration Flow for Oracle Privileged Account

No.	Task	Description
11	Upgrade the OPSS schema using Patch Set Assistant	For more information, see Section 3.2.9, "Upgrading OPSS Schema using Patch Set Assistant"
12	Configure the Database Security Store.	For more information, see Section 3.2.10, "Configuring Database Security Store for an Oracle Identity and Access Management Domain".
13	Complete the post-installation tasks.	Complete the following post-installation tasks: ■ Section 9.6, "Starting the Oracle WebLogic Administration Server" ■ Section 9.7, "Post-Installation Tasks" ■ Section 9.8, "Starting the Managed Server" ■ Section 9.9, "Assigning the Application Configurator Role to a User" ■ Section 9.10, "Optional: Setting Up Non-TDE Mode" ■ Section 9.11, "Optional: Configuring OPAM Console" ■ Section 9.12, "Verifying Oracle Privileged Account Manager" ■ Section 9.13, "Getting Started with Oracle Privileged Account Manager After Installation"

9.4 Optional: Enabling TDE in Oracle Privileged Account Manager Data Store

Oracle Privileged Account Manager can operate with Oracle Database TDE (Transparent Data Encryption) mode. You can choose to either enable or disable the TDE mode. Oracle strongly recommends to enable the TDE mode for enhanced security.

This section includes the following topics:

- Enabling TDE in the Database
- Enabling Encryption in OPAM Schema

9.4.1 Enabling TDE in the Database

For information about enabling Transparent Data Encryption (TDE) in the database for Oracle Privileged Account Manager, refer to the "Enabling Transparent Data Encryption" topic in *Oracle Database Advanced Security Administrator's Guide*.

For more information, see "Securing Stored Data Using Transparent Data Encryption" in the *Oracle Database Advanced Security Administrator's Guide*

After enabling TDE in the database for Oracle Privileged Account Manager, you must enable encryption in OPAM schema, as described in Section 9.4.2, "Enabling Encryption in OPAM Schema".

9.4.2 Enabling Encryption in OPAM Schema

To enable encryption in the OPAM schema, run the `opamxencrypt.sql` script with the OPAM schema user, using sqlplus or any other client.

IAM_HOME`/opam/sql/opamxencrypt.sql`

Example:

```
sqlplus DEV_OPAM/welcome1 @IAM_HOME/opam/sql/opamxencrypt.sql
```

9.5 Configuring Oracle Privileged Account Manager and Oracle Identity Navigator in a New WebLogic Domain

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

- Deployment Environment
- Components Deployed
- Dependencies
- Procedure

9.5.1 Deployment Environment

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

9.5.2 Components Deployed

Performing the configuration in this section deploys the Oracle Privileged Account Manager and Oracle Identity Navigator applications on a new WebLogic domain.

9.5.3 Dependencies

The configuration in this section depends on the following:

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

9.5.4 Procedure

Perform the following steps to configure Oracle Privileged Account Manager and Oracle Identity Navigator in a new WebLogic administration domain:

1. Start the Oracle Fusion Middleware Configuration Wizard by running the *IAM_HOME*`/common/bin/config.sh` script (on UNIX), or *IAM_HOME*`\common\bin\config.cmd` (on Windows).

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

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

2. On the Welcome screen, select **Create a new WebLogic domain**, and click **Next**. The Select Domain Source screen appears.
3. On the Select Domain Source screen, ensure that the **Generate a domain configured automatically to support the following products:** option is selected. Select **Oracle Privileged Account Manager - 11.1.2.0.0 [IAM_Home]**.

   > **Note:** When you select the **Oracle Privileged Account Manager - 11.1.2.0.0 [IAM_Home]** option, the following options are also selected, by default:
   >
   > - **Oracle Identity Navigator for Managed Server - 11.1.2.2.0 [IAM_Home]**
   > - **Oracle Platform Security Service 11.1.1.0 [IAM_Home]**
   > - **Oracle JRF 11.1.1.0 [oracle_common]**

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

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

   Select the desired options, and click **Next**.
9. Optional: Configure the following Administration Server parameters:
   - Name
   - Listen address

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

10. Optional: Configure Managed Servers, as required.
11. Optional: Configure Clusters, as required.

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

    Tip: Before configuring a machine, use the `ping` command to verify whether the machine or host name is accessible.
14. Optional: Assign the Administration Server to a machine.
15. Optional: Select Deployments, such as applications and libraries, and Services to target them to a particular cluster or server.
16. Optional: Configure RDBMS Security Store, as required.
17. On the Configuration Summary screen, 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 Privileged Account 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: After configuring Oracle Privileged Account Manager in a new WebLogic administration domain, you must complete the procedure described in the following sections, before starting the servers:

- Section 3.2.9, "Upgrading OPSS Schema using Patch Set Assistant"
- Section 3.2.10, "Configuring Database Security Store for an Oracle Identity and Access Management Domain"

9.6 Starting the Oracle WebLogic Administration Server

After installing and configuring Oracle Privileged Account Manager, you must start the Oracle WebLogic Administration Server, as described in Appendix C.1, "Starting the Stack".

9.7 Post-Installation Tasks

After installing and configuring Oracle Privileged Account Manager, you must run the `opam-config.sh` script (on UNIX), or `opam-config.bat` script (on Windows).

- Before executing the script, ensure that the WebLogic Administration Server is running. For more information on starting the Oracle WebLogic Administration Server, see Appendix C.1, "Starting the Stack".

  Note: If you are extending a domain, ensure that the WebLogic Administration Server is restarted before running the `opam-config.sh` script (on UNIX), or `opam-config.bat` script (on Windows).

- Set up `ANT_HOME`, `ORACLE_HOME`, `JAVA_HOME` and the `permgen` size.

  For example:

  On **Windows**:

  ```
  set ORACLE_HOME= ##set Oracle_Home here##
  set ANT_HOME=MW_HOME\modules\org.apache.ant_1.7.1
  set JAVA_HOME=MW_HOME\jdk160_14_R27.6.4-18
  set ANT_OPTS=-Xmx512M -XX:MaxPermSize=512m
  ```

  On **UNIX**:

  ```
  set ORACLE_HOME ##set Oracle_Home here##
  set ANT_HOME $MW_HOME/modules/org.apache.ant_1.7.1
  set JAVA_HOME $MW_HOME/jdk160_14_R27.6.5-32
  set ANT_OPTS "-Xmx512M -XX:MaxPermSize=512m"
  ```

  Note: On 64-bit platforms, when you install Oracle WebLogic Server using the generic jar file, JDK is not installed with Oracle WebLogic Server. You must install JDK separately, before installing Oracle WebLogic Server. In this case, you must specify the `JAVA_HOME` location accordingly.

- Go to *`IAM_HOME`*`/opam/bin` directory and run the `opam-config.sh` script (on UNIX), or `opam-config.bat` script (on Windows). Provide the following information, when prompted:
  - Oracle WebLogic Administration username
  - Oracle WebLogic Administration password
  - Oracle WebLogic Administration Server URL
  - Oracle WebLogic Domain Name

    Note: Oracle WebLogic Domain Name is case sensitive. You must provide the same value that you defined during domain creation.

  - Oracle Middleware Home

    Note: Oracle Middleware Home is case sensitive. You must provide the same value that you defined during domain creation.

- The log file for `opam-config` script will be created in *`MW_HOME`*`/user_projects/domains/`*`Domain_Name`*`/opam-config.log`.

If the above directory does not exist, then the log file for `opam-config` script will be created in *IAM_HOME*`/opam/config/opam-config.log`.

The log file location will be printed on the screen after the script is executed.

Note: After running the `opam-config.sh` script (on UNIX), or `opam-config.bat` script (on Windows), you must restart the Oracle WebLogic Administration Server, as described in Appendix C.1, "Starting the Stack".

9.8 Starting the Managed Server

You must start the Oracle Privileged Account Manager Managed Server, as described in Appendix C.1, "Starting the Stack".

9.9 Assigning the Application Configurator Role to a User

After you complete the installation process, you do not have any users with administrator roles. You may select a user and grant that user the Application Configurator role by using Oracle Identity Navigator.

Note: For more information, see "Assigning a Common Admin Role" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Navigator*.

For information about the Administration Roles that the Application Configurator user can have, see "Administration Role Types" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Privileged Account Manager*.

9.10 Optional: Setting Up Non-TDE Mode

Note: Oracle Privileged Account Manager can operate with Oracle Database TDE (Transparent Data Encryption) mode. You can choose to either enable or disable the TDE mode. Oracle strongly recommends to enable the TDE mode for enhanced security.

If you want to disable TDE mode, you must set the flag `tdemode` to `false`.

Note: The steps described in this section are required only if you choose to skip Section 9.4, "Optional: Enabling TDE in Oracle Privileged Account Manager Data Store".

Complete the following steps to disable TDE mode:

1. Set the environment variables `ORACLE_HOME` and `JAVA_HOME`.
2. Run the following script:

   On **Windows**:

```
ORACLE_HOME\opam\bin\opam.bat -url OPAM_Server_URL -x modifyglobalconfig
-propertyname tdemode -propertyvalue false -u OPAM_APPLICATION_CONFIGURATOR_
```

```
USER -p Password
```

where OPAM_Server_URL is of the form https://*OPAM_Managed_Server_Hostname:OPAM_Managed_Server_SSL_port*/opam

On **UNIX**:

```
ORACLE_HOME/opam/bin/opam.sh -url OPAM_Server_Url -x modifyglobalconfig
-propertyname tdemode -propertyvalue false -u OPAM_APPLICATION_CONFIGURATOR_
USER -p Password
```

where OPAM_Server_URL is of the form https://*OPAM_Managed_Server_Hostname:OPAM_Managed_Server_SSL_port*/opam

---

Note: TDE mode can be enabled or disabled at any point after installing and configuring Oracle Privileged Account Manager. For more information on changing the TDE mode at a later time, refer to the "Securing Data On Disk" topic in the *Oracle Fusion Middleware Administrator's Guide for Oracle Privileged Account Manager*.

9.11 Optional: Configuring OPAM Console

When the Application Configurator user logs in using the following URL:

```
http://<opam-managedserver-host>:<opam-managedserver-nonsslport>/oinav/opam
```

the Oracle Privileged Account Manager Console autodetects the connection settings for the Oracle Privileged Account Manager server, and the Oracle Privileged Account Manager Console is populated with content.

To modify the server connection settings, the Application Configurator user can go to the **Configuration** option on the left pane, and click on **Server Connection**. On the Server Connection tab, the user can provide a new host and port.

9.12 Verifying Oracle Privileged Account Manager

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

1. Ensure that the Oracle Privileged Account Manager Server is up and running, using the following URL:

   ```
   https://<opam-managedserver-host>:<opam-managedserver-sslport>/opam
   ```

   You will be prompted to enter a username and password. Enter your WebLogic username and password. The following result should be displayed:

   ```
   {
     ServerState: {
       Status: "Oracle Privileged Account Manager Server is up!",
       StatusCode: 0
     },
     Requestor: "WebLogic_username",
     RequestorGroups: [
       "Administrators"
     ]
   }
   ```

2. Log in to the Administration Console for Oracle Privileged Account Manager using the URL:

   `http://<opam-managedserver-host>:<opam-managedserver-nonsslport>/oinav/opam`

   When you access this Administration Console running on the OPAM Managed 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 Privileged Account Manager is successful, this console shows `opam_server1` in the running mode, which is the default Managed Server.

4. In the Domain Structure pane, click on **Deployments**. The following applications should be listed in the Deployments table, and the state must be `Active`:

   - `oinav`
   - `opam`
   - `opamsessionmgr`

9.13 Getting Started with Oracle Privileged Account Manager After Installation

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

10

Configuring Oracle Access Management Mobile and Social

This chapter explains how to configure Oracle Access Management Mobile and Social. It includes the following topics:

- Overview
- Important Note Before You Begin
- Installation and Configuration Roadmap for Oracle Access Management Mobile and Social
- Configuring Oracle Access Management Mobile and Social with Oracle Access Manager
- Verifying Oracle Access Management Mobile and Social
- Getting Started with Oracle Access Management Mobile and Social After Installation

10.1 Overview

For an introduction to the Oracle Access Management Mobile and Social, see the "Understanding Mobile and Social" chapter in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.

10.2 Important Note Before You Begin

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

10.3 Installation and Configuration Roadmap for Oracle Access Management Mobile and Social

Table 10–1 lists the tasks for installing and configuring Oracle Access Management Mobile and Social.

Table 10–1 Installation and Configuration Flow for Oracle Access Management Mobile and Social

No.	Task	Description
1	Review installation concepts in the Installation Planning Guide.	Read the *Oracle Fusion Middleware Installation Planning Guide*, which describes the process for various users to install or upgrade to Oracle Fusion Middleware 11*g* (11.1.2) depending on the user's existing environment.
2	Review the system requirements and certification documents to ensure that your environment meets the minimum installation requirements for the components you are installing.	For more information, see Section 2.1, "Reviewing System Requirements and Certification".
3	Obtain the Oracle Fusion Middleware Software.	For more information, see Section 3.2.1, "Obtaining the Oracle Fusion Middleware Software"
4	Review the Database requirements.	For more information, see Section 3.2.2, "Database Requirements".
5	Run Oracle Fusion Middleware Repository Creation Utility (RCU) to create and load the appropriate schemas for Oracle Identity and Access Management products.	For more information, see Section 3.2.3, "Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU)". **Note:** If you are configuring Oracle Access Management Mobile and Social standalone, skip this step.
6	Review WebLogic Server and Middleware Home requirements.	For more information, see Section 3.2.4, "WebLogic Server and Middleware Home Requirements".
7	Start the Oracle Identity and Access Management Installer.	For more information, see Section 3.2.6, "Starting the Oracle Identity and Access Management Installer".
8	Install the Oracle Identity and Access Management 11*g* software.	Oracle Access Management Mobile and Social is included in the Oracle Identity and Access Management Suite. You can use the Oracle Identity and Access Management 11*g* Installer to install Oracle Identity and Access Management Suite. For more information, see Section 3.2.7, "Installing Oracle Identity and Access Management 11g Release 2 (11.1.2.2.0)".
9	Run the Oracle Fusion Middleware Configuration Wizard to configure your Oracle Identity and Access Management products in a new or existing WebLogic domain.	For more information, see Section 10.4, "Configuring Oracle Access Management Mobile and Social with Oracle Access Manager"
10	Configure the Database Security Store.	For more information, see Section 3.2.10, "Configuring Database Security Store for an Oracle Identity and Access Management Domain". **Note:** If you are configuring Oracle Access Management Mobile and Social standalone, skip this step.
11	Start the servers.	You must start the Administration Server and all Managed Servers. For more information, see Appendix C.1, "Starting the Stack".
12	Complete the post-installation tasks.	Complete the following post-installation tasks: ■ Section 10.5, "Verifying Oracle Access Management Mobile and Social" ■ Section 10.6, "Getting Started with Oracle Access Management Mobile and Social After Installation"

10.4 Configuring Oracle Access Management Mobile and Social with Oracle Access Manager

This topic describes how to configure Oracle Access Management Mobile and Social with Oracle Access Manager. It includes the following sections:

- Overview
- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure

10.4.1 Overview

Oracle Access Management Mobile and Social is packaged with Oracle Access Management. Oracle Access Management has many components, such as Oracle Access Manager, Oracle Access Management Security Token Service, Oracle Access Management Identity Federation, and Oracle Access Management Mobile and Social. In this scenario, only Oracle Access Manager is enabled as the authentication provider, by default. You can enable other services like Oracle Access Management Mobile and Social using the Oracle Access Management Administration Console, after the installation is complete.

10.4.2 Appropriate Deployment Environment

Perform the configuration described in this section if you want to use Oracle Access Management Mobile and Social as an Oracle Access Manager service.

In this configuration, you can select other Oracle Identity and Access Management products like Oracle Adaptive Access Manager when you configure Oracle Access Management Mobile and Social.

10.4.3 Components Deployed

Performing the configuration in this section deploys the following Oracle Access Management components:

- Oracle Access Manager
- Oracle Access Management Security Token Service
- Oracle Access Management Identity Federation
- Oracle Access Management Mobile and Social

10.4.4 Dependencies

The configuration in this section depends on the following:

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

10.4.5 Procedure

Perform the following steps to configure Oracle Access Management Mobile and Social and Oracle Access Manager in a new WebLogic administration domain:

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

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

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

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

3. On the Select Domain Source screen, ensure that the **Generate a domain configured automatically to support the following products:** option is selected. Select **Oracle Access Management - 11.1.2.0.0 [IAM_Home]**.

   Note: When you select the **Oracle Access Management - 11.1.2.0.0 [IAM_Home]** option, the following options are also selected, by default:

   - **Oracle Platform Security Service 11.1.1.0 [IAM_Home]**
   - **Oracle JRF 11.1.1.0 [oracle_common]**

   You may optionally select **Oracle Adaptive Access Manager Admin Server - 11.1.2.0.0 [IAM_Home]** if you want to add Oracle Adaptive Access Manager to the same WebLogic Administration domain containing Oracle Access Management Mobile and Social.

   Oracle highly recommends that you select Oracle Adaptive Access Manager for using device registration feature.

   Note: If you select the **Oracle Adaptive Access Manager Admin Server - 11.1.2.0.0 [IAM_Home]** option, the following options are also selected, by default:

   - **Oracle Enterprise Manager 11.1.1.0 [oracle_common]**
   - **Oracle Identity Navigator - 11.1.2.0.0 [IAM_Home]**

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

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

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

6. Choose a JDK 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.
7. On the Configure JDBC Component Schema screen, select a component schema, such as the **OAM Infrastructure Schema** or the **OPSS Schema**, that you want to modify.

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

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

    Tip: Before configuring a machine, use the `ping` command to verify whether the machine or host name is accessible.
14. Optional: Assign the Administration Server to a machine.
15. Optional: Select Deployments, such as applications and libraries, and Services to target them to a particular cluster or server.
16. Optional: Configure RDBMS Security Store, as required.
17. On the Configuration Summary screen, 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 Access Management Mobile and Social with 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.

Note: After configuring Oracle Access Management Mobile and Social with Oracle Access Management in a new WebLogic administration domain, you must configure the Database Security Store. For more information, see Section 3.2.10, "Configuring Database Security Store for an Oracle Identity and Access Management Domain".

18. Start the Oracle WebLogic Administration Server, as described in Appendix C.1, "Starting the Stack".
19. Start all Managed Servers, as described in Appendix C.1, "Starting the Stack".

Note: After you configure Oracle Access Management Mobile and Social with Oracle Access Management, only Oracle Access Manager is enabled as the authentication provider, by default. To enable other Oracle Access Management components, such as OSTS, OIF, and Oracle Access Management Mobile and Social, refer to "Enabling or Disabling Available Services" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.

10.5 Verifying Oracle Access Management Mobile and Social

After completing the installation process, you can verify the installation and configuration of Oracle Access Management Mobile and Social 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 Management 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. From the Oracle Access Management console, go to **System Configuration** tab>**Common Configuration** section>**Available Services** node.

   If you have configured Oracle Access Management Mobile and Social with Oracle Access Management, you must enable the **Status** of Mobile and Social and ensure that the **Status** of Mobile and Social has a green check mark.

   If you have configured Oracle Access Management Mobile and Social standalone, ensure that the **Status** of Mobile and Social has a green check mark.

10.6 Getting Started with Oracle Access Management Mobile and Social After Installation

After installing Oracle Access Management Mobile and Social, refer to the "Mobile and Social System Configuration and Administration" chapter in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.

11 Lifecycle Management

This chapter explains how to address situations where a lifecycle change event occurs for an Oracle Identity and Access Management component that is integrated with one or more components.

Topics include:

- How Lifecycle Events Impact Integrated Components
- LCM for Oracle Identity Manager
- LCM for Oracle Access Manager
- LCM for Oracle Adaptive Access Manager
- LCM for Oracle Identity Navigator
- References

11.1 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.

11.2 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 Target Environment" in the *Oracle Fusion Middleware Administrator's Guide*
- "Move Oracle Identity Manager to an Existing Target Environment" in the *Oracle Fusion Middleware Administrator's Guide*

11.3 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 Oracle Access Manager:

- "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 11*g* Data from a Test to a Production Deployment" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager*

11.4 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 Oracle Adaptive Access Manager:

- "Adding a Component Link to the Product Launcher by Using Product Discovery" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Navigator*
- "Oracle Virtual Directory (OVD) Rewiring with Existing Oracle Adaptive Access Manager (OAAM)" in the *Oracle Fusion Middleware Developer's Guide for Oracle Adaptive Access Manager*
- "Oracle Identity Manager (OIM) Rewiring with Existing Oracle Adaptive Access Manager (OAAM)" in the *Oracle Fusion Middleware Developer's Guide for Oracle Adaptive Access Manager*
- "OID Rewiring with Existing OAAM (in Cases without OVD)" in the *Oracle Fusion Middleware Developer's Guide for Oracle Adaptive Access Manager*
- "Database Rewiring with Existing OAAM" in the *Oracle Fusion Middleware Developer's Guide for Oracle Adaptive Access Manager*
- "Move Oracle Adaptive Access Manager to a New Target Environment" in the *Oracle Fusion Middleware Administrator's Guide*
- "Move Oracle Adaptive Access Manager to an Existing Target Environment" in the *Oracle Fusion Middleware Administrator's Guide*

11.5 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 Oracle Identity Navigator:

- "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*

11.6 References

For additional information about lifecycle management in Oracle Fusion Middleware, see "Part V Advanced Administration: Expanding Your Environment" in the *Oracle Fusion Middleware Administrator's Guide*.

Part III

Appendixes

Part III contains the following appendixes:

- Appendix A, "Oracle Identity and Access Management 11g Release 2 (11.1.2.2.0) Software Installation Screens"
- Appendix B, "Oracle Identity Manager Configuration Screens"
- Appendix C, "Starting or Stopping the Oracle Stack"
- Appendix D, "Preconfiguring Oracle Directory Server Enterprise Edition (ODSEE)"
- Appendix E, "Preconfiguring Oracle Unified Directory (OUD)"
- Appendix F, "Preconfiguring Oracle Internet Directory (OID)"
- Appendix G, "Preconfiguring Active Directory"
- Appendix H, "Creating Oracle Entitlement Server Schemas for Apache Derby"
- Appendix I, "Configuring the PDP Proxy Client for Web Service Security Module"
- Appendix J, "Deinstalling and Reinstalling Oracle Identity and Access Management"
- Appendix K, "Troubleshooting the Installation"
- Appendix L, "Oracle Adaptive Access Manager Partition Schema Reference"
- Appendix M, "Software Deinstallation Screens"

A

Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0) Software Installation Screens

This appendix describes the screens of the Oracle Identity and Access Management 11*g* software Installation Wizard that enables you to install Oracle Identity Manager, Oracle Access Management, Oracle Adaptive Access Manager, Oracle Entitlements Server, Oracle Identity Navigator, Oracle Privileged Account Manager, and Oracle Access Management Mobile and Social.

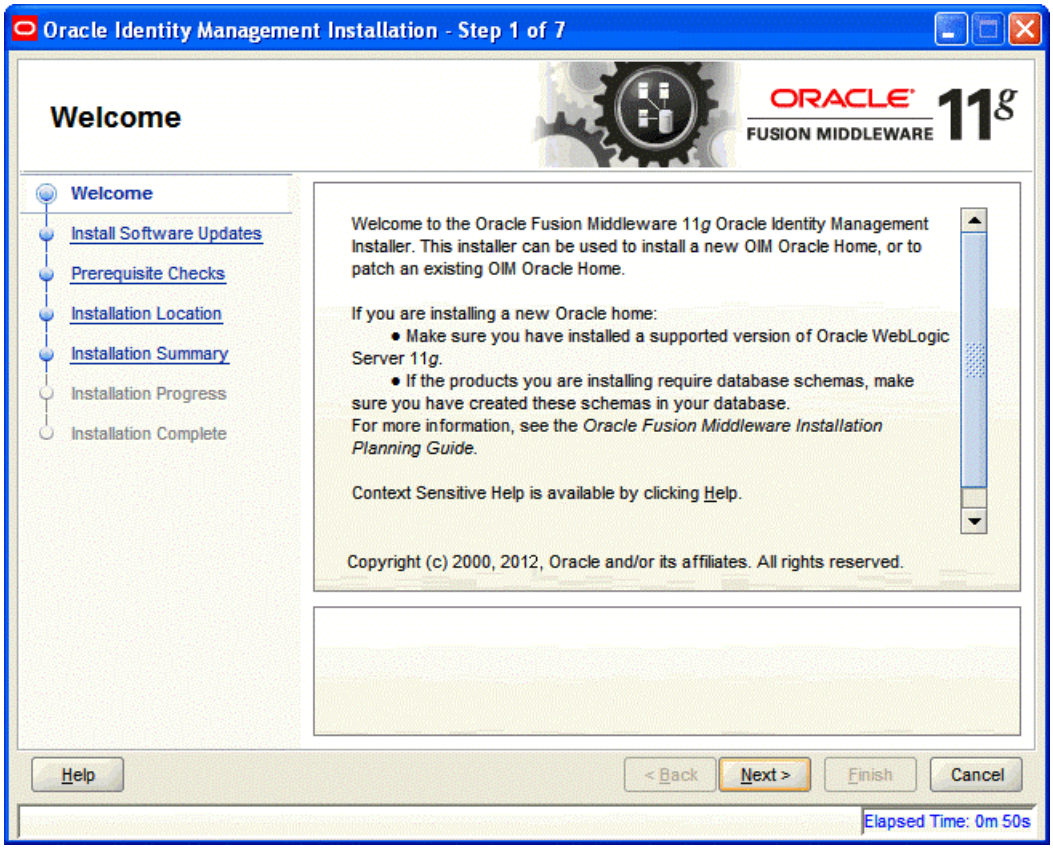
It contains the following topics:

- Welcome
- Install Software Updates
- Prerequisite Checks
- Specify Installation Location
- Installation Summary
- Installation Progress
- Installation Complete

A.1 Welcome

The Welcome screen is displayed each time you start the Oracle Identity and Access Management 11*g* Installer wizard.

Figure A–1 Welcome Screen

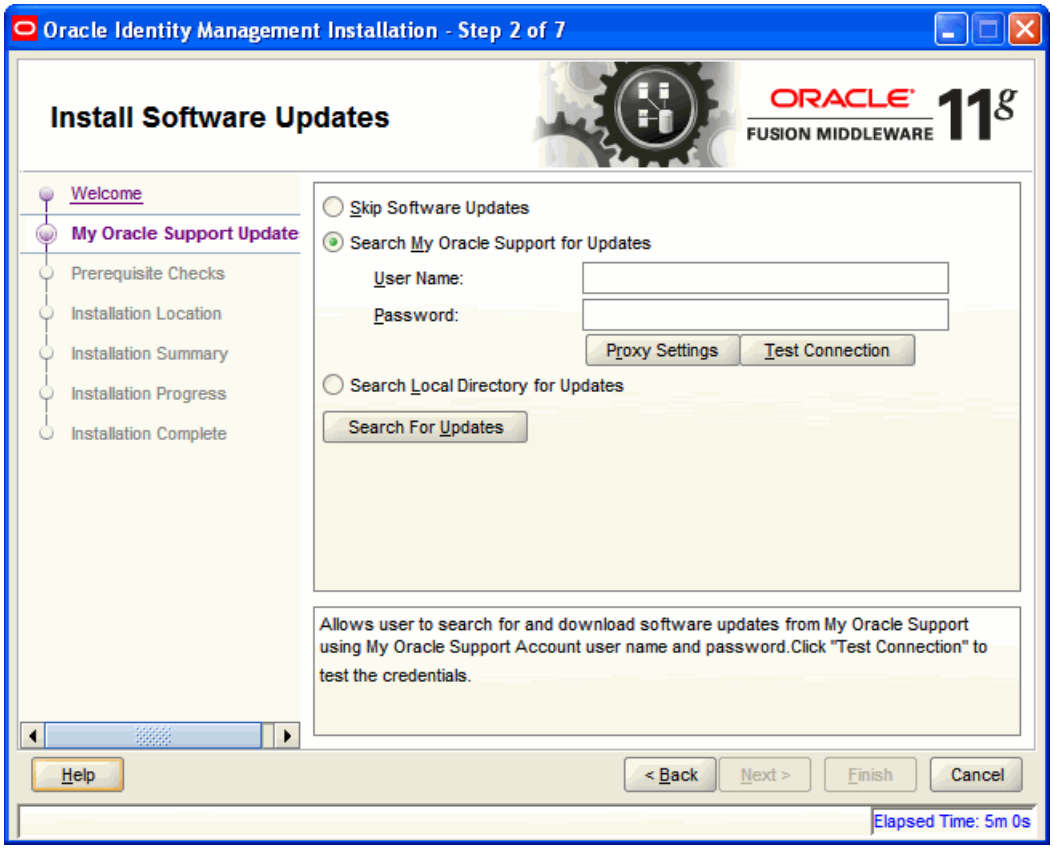


Click **Next** to continue.

A.2 Install Software Updates

This screen helps to quickly and easily search for the latest software updates, including important security updates, via your My Oracle Support account.

Figure A–2 Install Software Updates

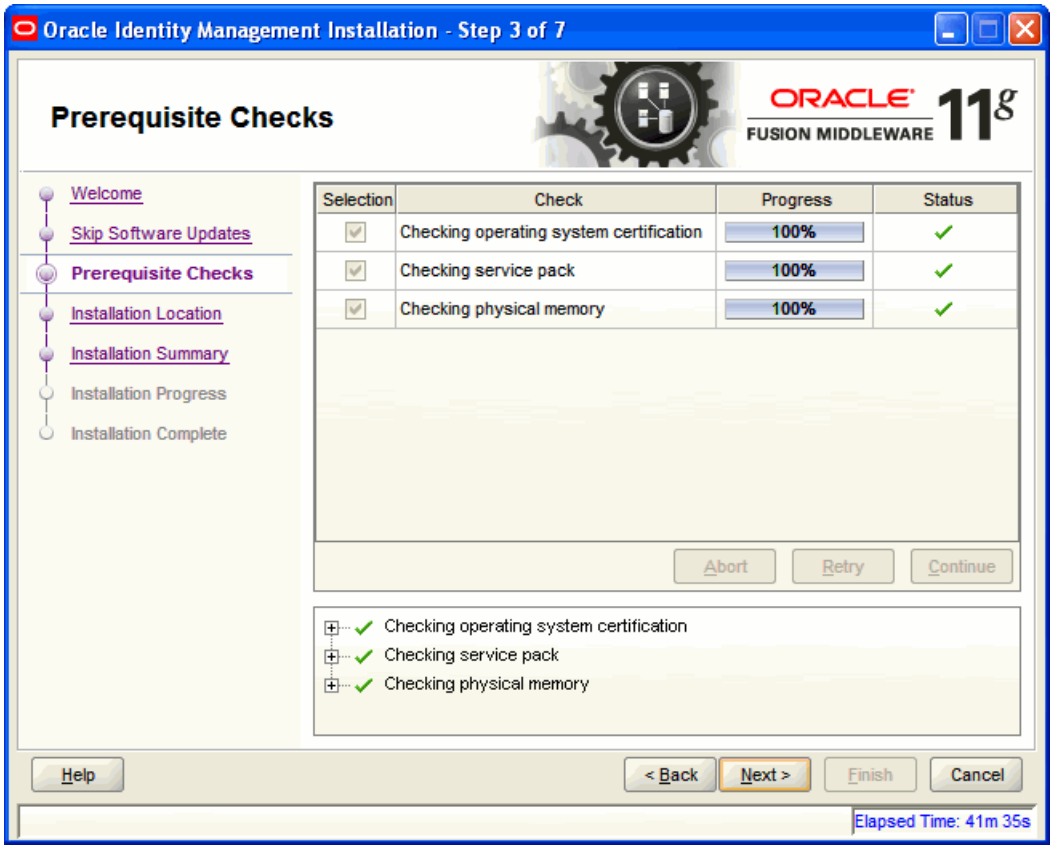


A.3 Prerequisite Checks

The installation program ensures that you have a certified version, the correct software packages, sufficient space and memory to perform the operations that you have selected. If any issues are detected, errors appear on this page.

The following example screen applies to Windows operating systems only.

Figure A–3 Prerequisite Checks Screen



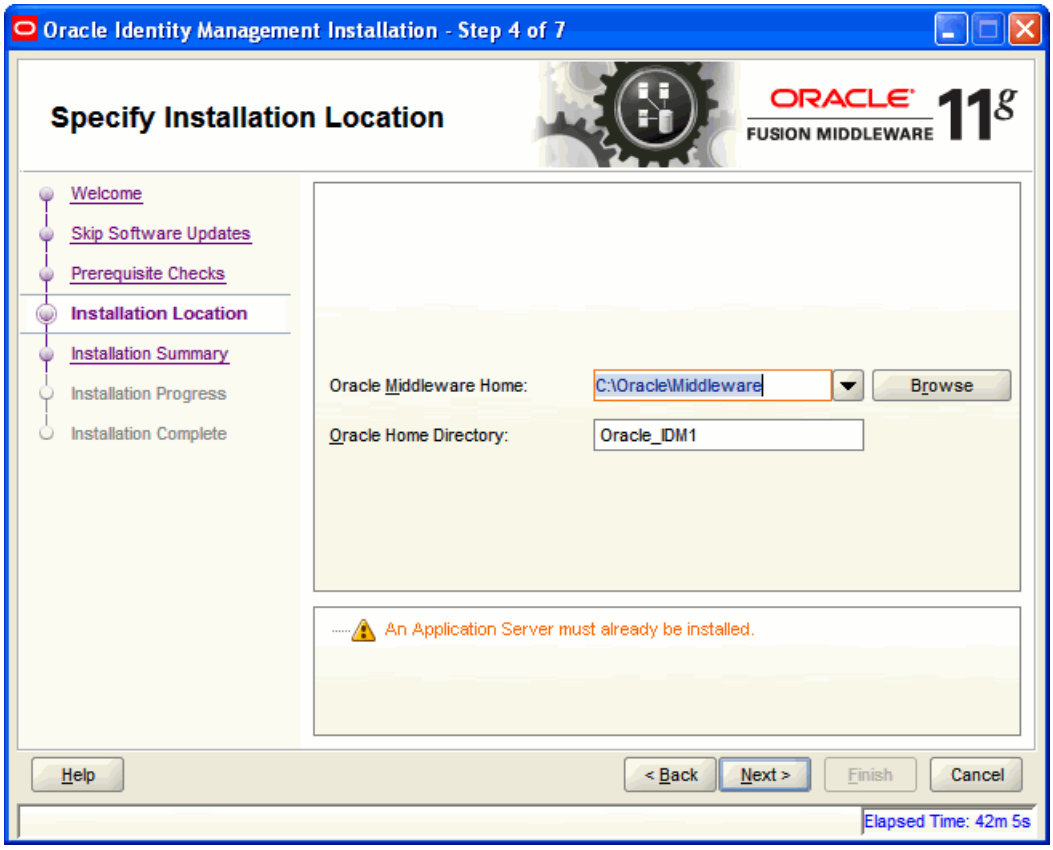
On this screen, you can select to **Abort**, **Retry**, or **Continue** with the installation.

If all the prerequisite checks pass inspection, click **Next** to continue.

A.4 Specify Installation Location

In this screen, you enter a location for the new Oracle Identity and Access Management 11*g* software being installed.

Figure A–4 Specify Installation Location Screen



Ensure that Oracle WebLogic Server is already installed on your machine. Navigate to the Oracle Fusion Middleware Home directory by clicking **Browse**. Enter a name for the new Oracle Home directory for Oracle Identity and Access Management 11g components.

If the Middleware location does not exist, you must install WebLogic Server and create a Middleware Home directory, as described in Section 3.2.4, "WebLogic Server and Middleware Home Requirements", before running the Oracle Identity and Access Management Installer.

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

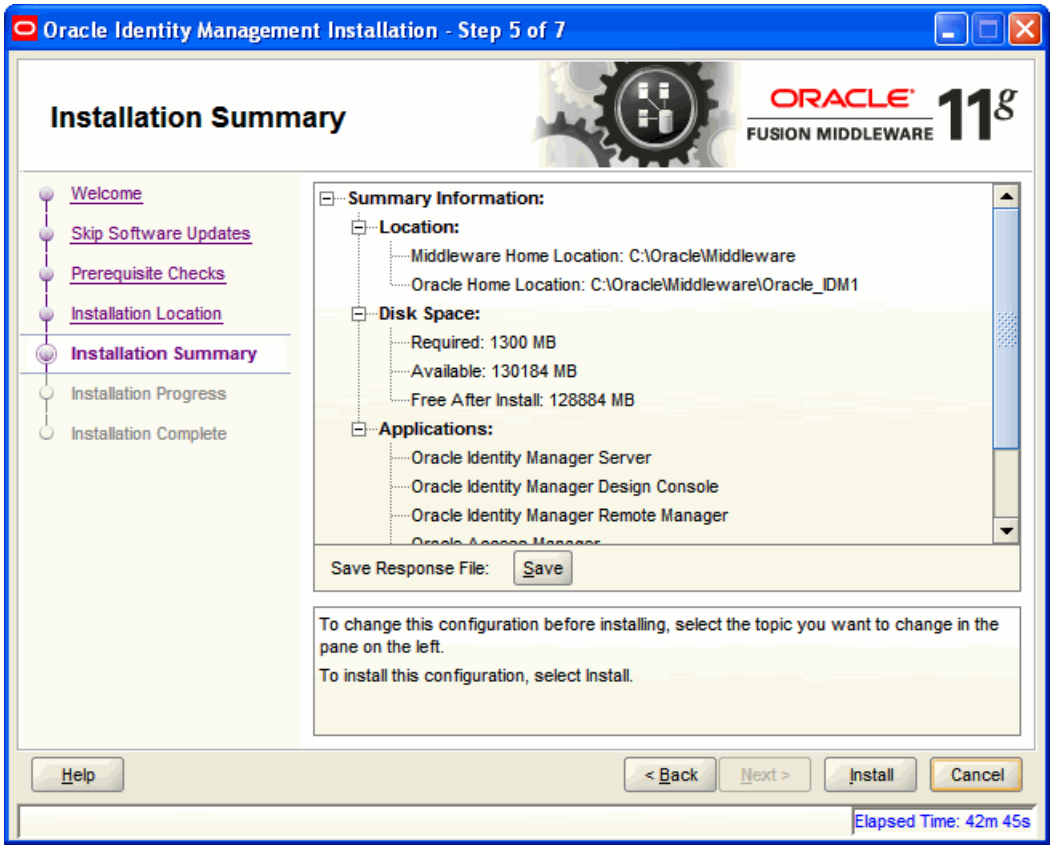
If you want to install only Oracle Identity Manager Design Console or Remote Manager, you do not need to install Oracle WebLogic Server or create a Middleware Home directory on the machine where Design Console or Remote Manager is being configured.

Click **Next** to continue.

A.5 Installation Summary

This screen displays a summary of your Oracle Identity and Access Management 11*g* installation.

Figure A–5 Installation Summary Screen

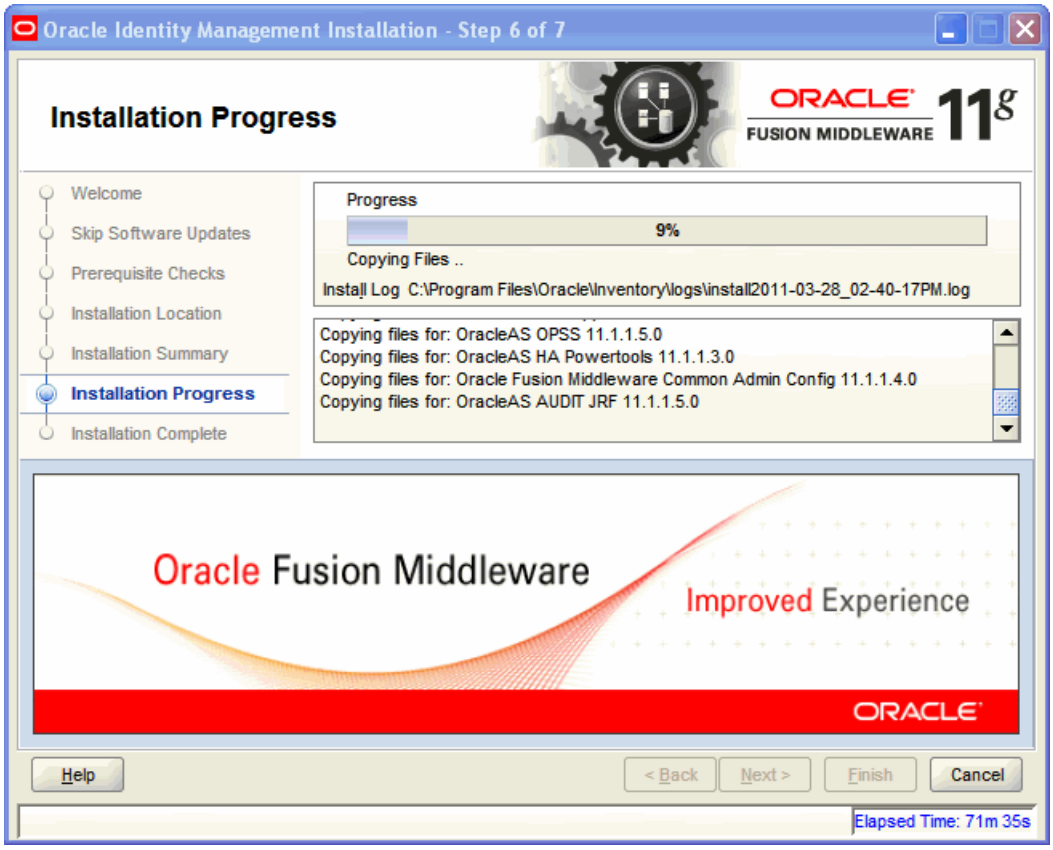


Review the contents of this screen, and click **Install** to start installing the Oracle Identity and Access Management 11*g* software.

A.6 Installation Progress

This screen displays the progress of the Oracle Identity and Access Management installation.

Figure A–6 Installation Progress Screen

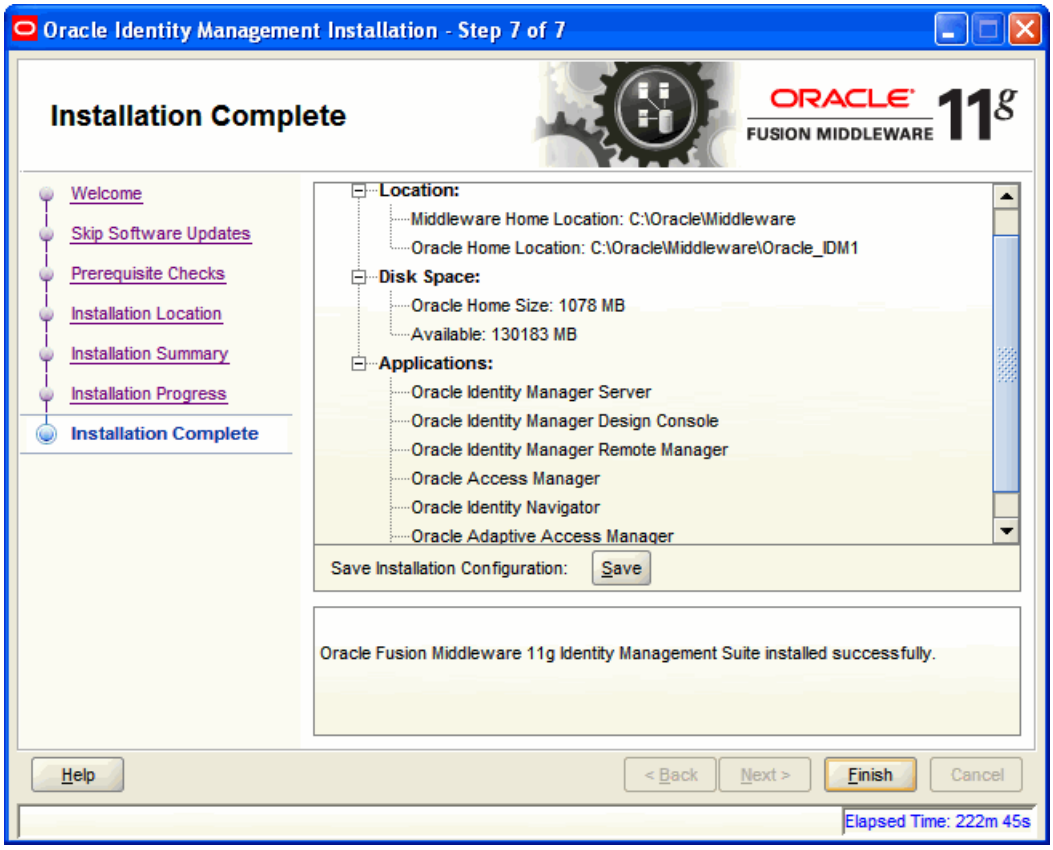


If you want to quit before the installation is completed, click **Cancel**. The installation progress indicator gives a running inventory of the files that are being installed. If you are only installing the software binaries, installation is complete after all of the binaries have been installed.

A.7 Installation Complete

This screen displays a summary of the installation parameters, such as Location, Disk Space, and Applications. To save the installation configuration in a response file, which is used to perform silent installations, click **Save**.

Figure A–7 Installation Complete Screen



Click **Finish** to complete the installation process.

B

Oracle Identity Manager Configuration Screens

This appendix describes the screens of the Oracle Identity Manager 11*g* Configuration Wizard that enables you to configure Oracle Identity Manager Server, Oracle Identity Manager Design Console, and Oracle Identity Manager Remote Manager.

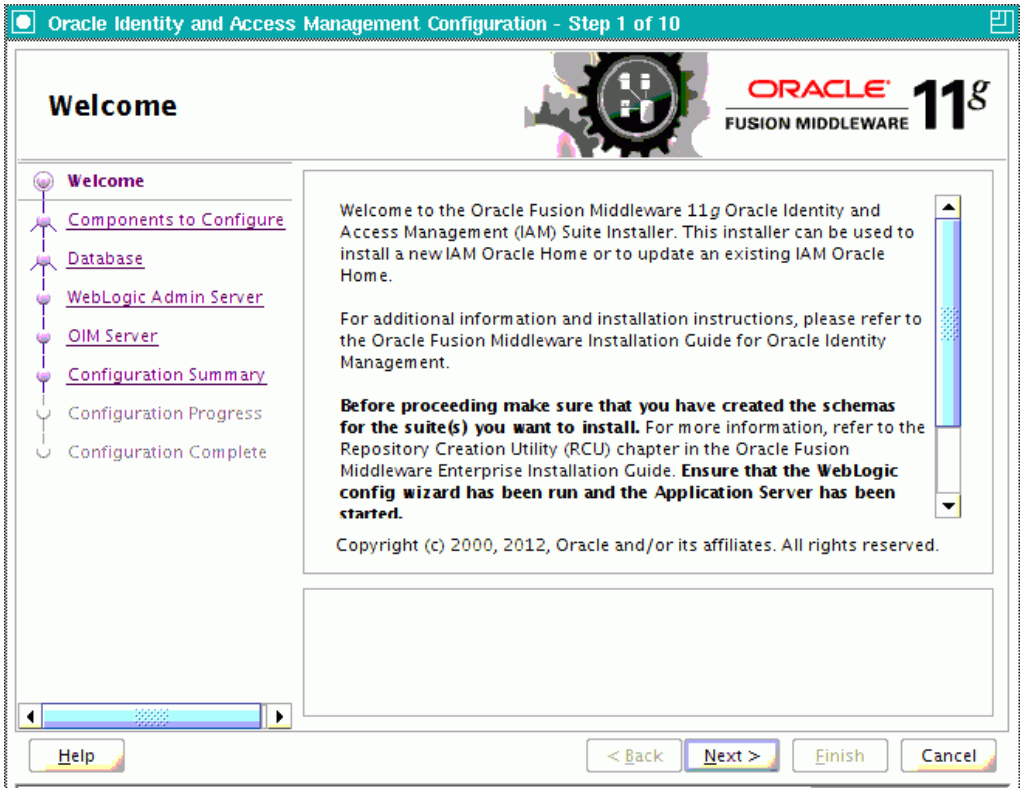
This appendix contains the following topics:

- Welcome
- Components to Configure
- Database
- WebLogic Admin Server
- OIM Server
- LDAP Server
- LDAP Server Continued
- Configuration Summary

B.1 Welcome

The Welcome screen is displayed each time you start the Oracle Identity Manager Configuration Wizard.

Figure B–1 Welcome Screen



You can use the Oracle Identity Manager Configuration Wizard only once during initial setup for configuring Oracle Identity Manager Server. After configuring Oracle Identity Manager Server using this wizard, you cannot re-run this wizard to modify the configuration of Oracle Identity Manager. You must use Oracle Enterprise Manager Fusion Middleware Control to make such modifications. However, you can run this wizard on other machines, where Design Console or Remote Manager is configured, as and when needed.

Ensure that you have configured Oracle Identity Manager in a new or existing WebLogic domain before launching the Oracle Identity Manager Configuration Wizard to configure Oracle Identity Manager Server, Design Console on Windows, and Remote Manager.

If you are configuring Server, you must run this wizard on the machine where the WebLogic Administration Server is running (the Administration Server for the domain in which Oracle Identity Manager is deployed). Ensure that the Administration Server is up and running before you start configuring Oracle Identity Manager Server.

If you are configuring only Design Console, you must run this wizard on the Windows machine where Design Console should be configured. If you are configuring only Remote Manager, you must run this wizard on the machine where Remote Manager is being configured. Note that the Oracle Identity Manager Server should be configured before you can configure Design Console or Remote Manager.

Click **Next** to continue.

B.2 Components to Configure

Use this screen to select the Oracle Identity Manager components that you want to configure. Oracle Identity Manager components include Server, Design Console, and Remote Manager.

Before configuring Oracle Identity Manager Server, Design Console or Remote Manager, ensure that you have configured Oracle Identity Manager in a new or existing WebLogic domain using the Oracle Fusion Middleware Configuration Wizard.

Figure B–2 Components to Configure Screen

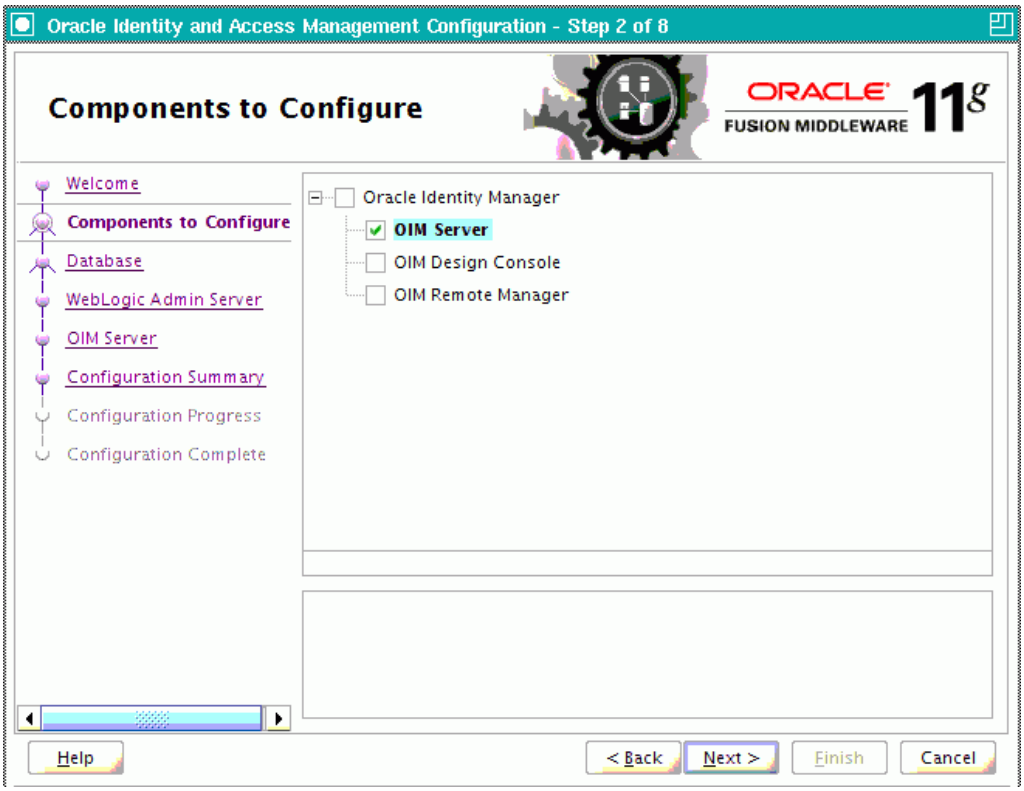


Table B–1 describes the Oracle Identity Manager components that you can choose.

Table B–1 Oracle Identity Manager Configuration Choices

Option	Description
Configure all components on this screen	To configure Oracle Identity Manager Server, Design Console, and Remote Manager simultaneously on the same machine, select the **Oracle Identity Manager** option.
Configure only Oracle Identity Manager Server	To configure only Oracle Identity Manager Server, select the **OIM Server** option. This option is selected, by default. Note that WebLogic Administration Server for the domain (the domain in which Oracle Identity Manager is deployed) should be up and running.
Configure only Oracle Identity Manager Design Console	To configure only Oracle Identity Manager Design Console, select the **OIM Design Console** option. However, note that Oracle Identity Manager Server must be configured either on the local machine or on a remote machine before you can run Design Console on development machines. Design Console is supported on Windows operating systems only.

Table B–1 (Cont.) Oracle Identity Manager Configuration Choices

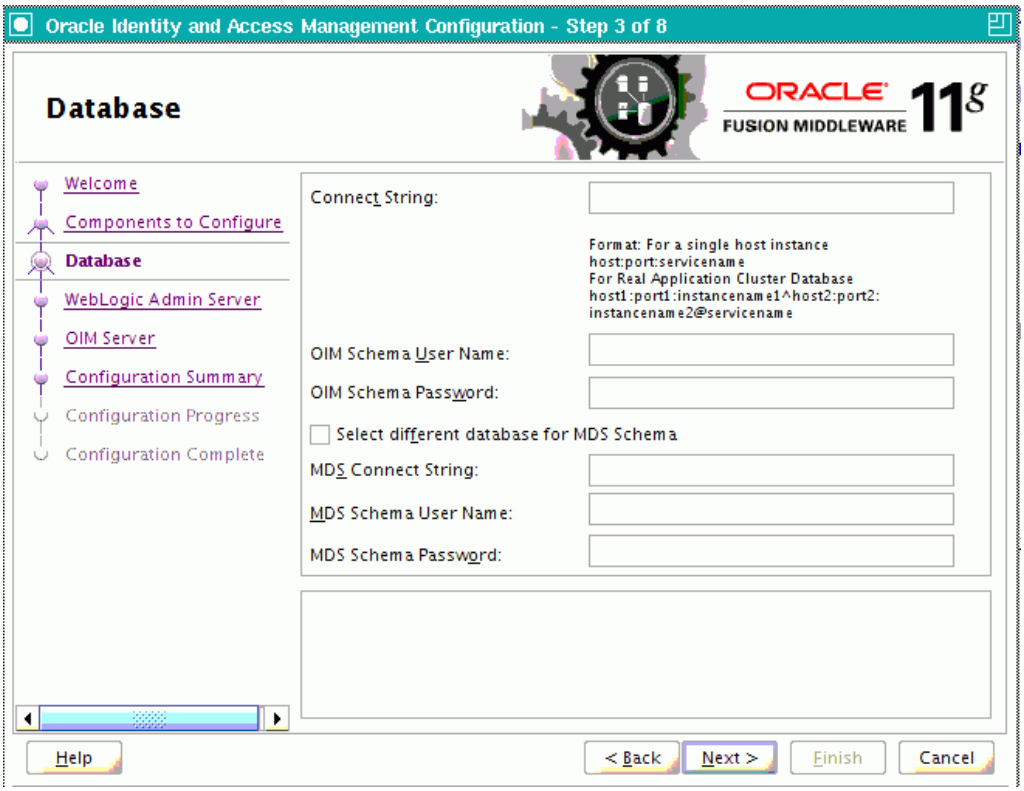
Option	Description
Configure only Oracle Identity Manager Remote Manager	To configure only Oracle Identity Manager Remote Manager, select the **OIM Remote Manager** option. However, note that Oracle Identity Manager Server must be configured either on the local machine or on a remote machine before you can run Remote Manager.

Note: You can also select any combination of two of the three Oracle Identity Manager components.

B.3 Database

In this screen, you specify the database and schema information. Note that you should have created and loaded Oracle Identity Manager schemas using the Oracle Fusion Middleware Repository Creation Utility (RCU) before configuring Oracle Identity Manager Server. For information about creating and loading Oracle Identity Manager schemas, see Section 3.2.3, "Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU)".

Figure B–3 Database Screen



You can use the same database or different databases for creating the Oracle Identity Manager schema and the Metadata Services schema.

Table B–2 describes the database connection information that you must specify.

Table B–2 Fields in the Database Screen

Field	Description

Connect String	Enter the full path, listen port, and service name for your Oracle database. For a single host instance, the format of connect string is `hostname:port:servicename`.
	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`

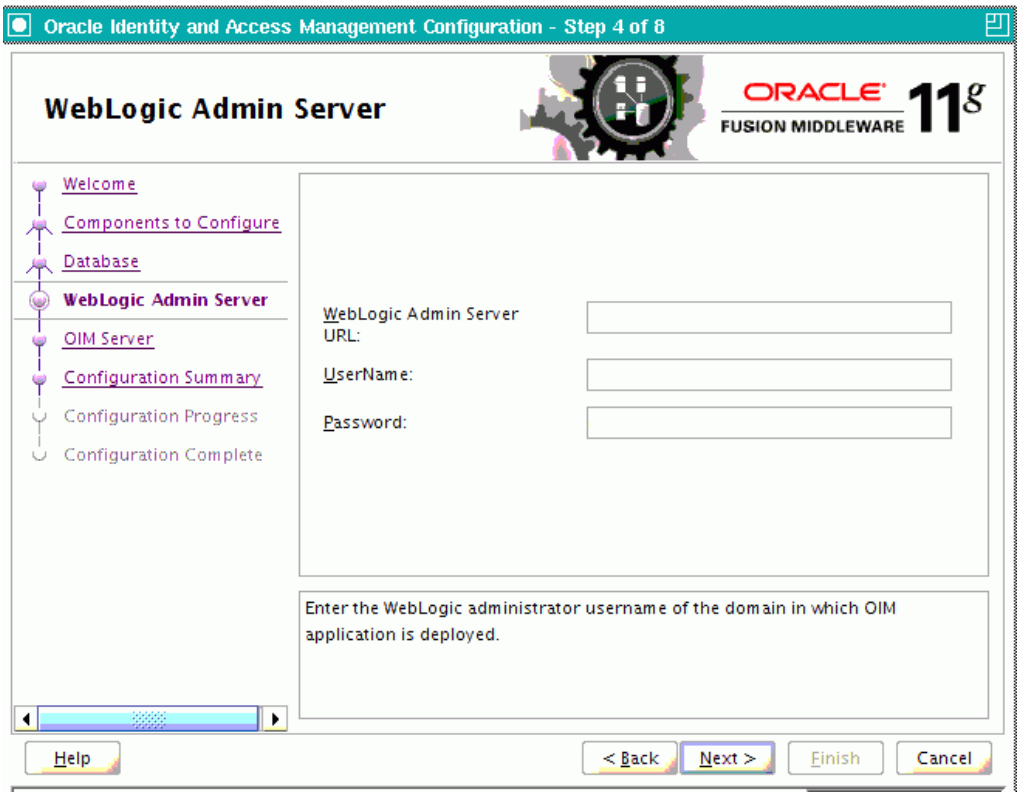
OIM Schema User Name	Enter the name of the schema user that you created for Oracle Identity Manager using the Oracle Fusion Middleware Repository Creation Utility. If you upgraded your existing Oracle Identity Manager schema to 11*g* Release 1 (11.1.1), enter the user name for your existing schema.
OIM 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.
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.

B.4 WebLogic Admin Server

In this screen, you specify the t3 URL, user name and password for the WebLogic administration domain in which the Oracle Identity Manager application is deployed. Ensure that the Administration Server is up and running.

Figure B–4 WebLogic Admin Server Screen



In the **WebLogic Admin Server URL** text box, enter the t3 URL of the Administration Server for the WebLogic domain in the following format:

`t3://hostname:port`

In the **UserName** text box, enter the WebLogic Administrator user name.

In the **Password** text box, enter the WebLogic Administrator password.

After entering information in the fields, click **Next** to continue.

B.5 OIM Server

Use this screen to set a password for the for the system administrator (`xelsysadm`).

Figure B–5 OIM Server Screen

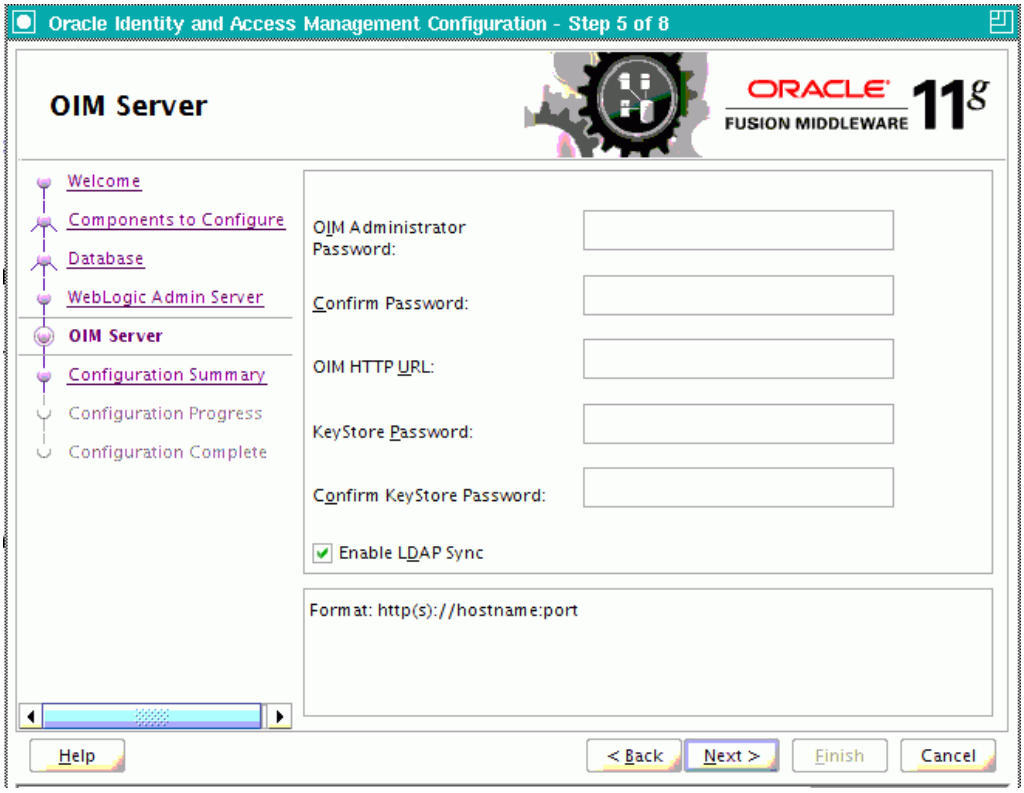


Table B–3 describes the Oracle Identity Manager Server parameters that you can configure.

Table B–3 Oracle Identity Manager Server Configuration Parameters

Field Name	Description
OIM Administrator Password	Enter a new password for the administrator. 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.

Table B–3 (Cont.) Oracle Identity Manager Server Configuration Parameters

Field Name	Description
Confirm KeyStore Password	Enter the new password again to confirm.

Enabling OIM-LDAP Synchronization

In this screen, you can enable synchronization of Oracle Identity Manager roles, users, and their hierarchy to an LDAP directory.

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 Section 5.9.5, "Completing the Prerequisites for Enabling LDAP Synchronization". After completing the prerequisites for enabling LDAP Synchronization, select the **Enable LDAP Sync** option.

After entering information in the fields, click **Next** to continue.

B.6 LDAP Server

This screen is displayed only if you select the **Enable LDAP Sync** option on the BI Publisher screen. In the LDAP Server screen, you should specify the authentication information for the Directory Server, as you want to synchronize Oracle Identity Manager roles, users, and their hierarchy to an LDAP directory.

Figure B–6 LDAP Server Screen

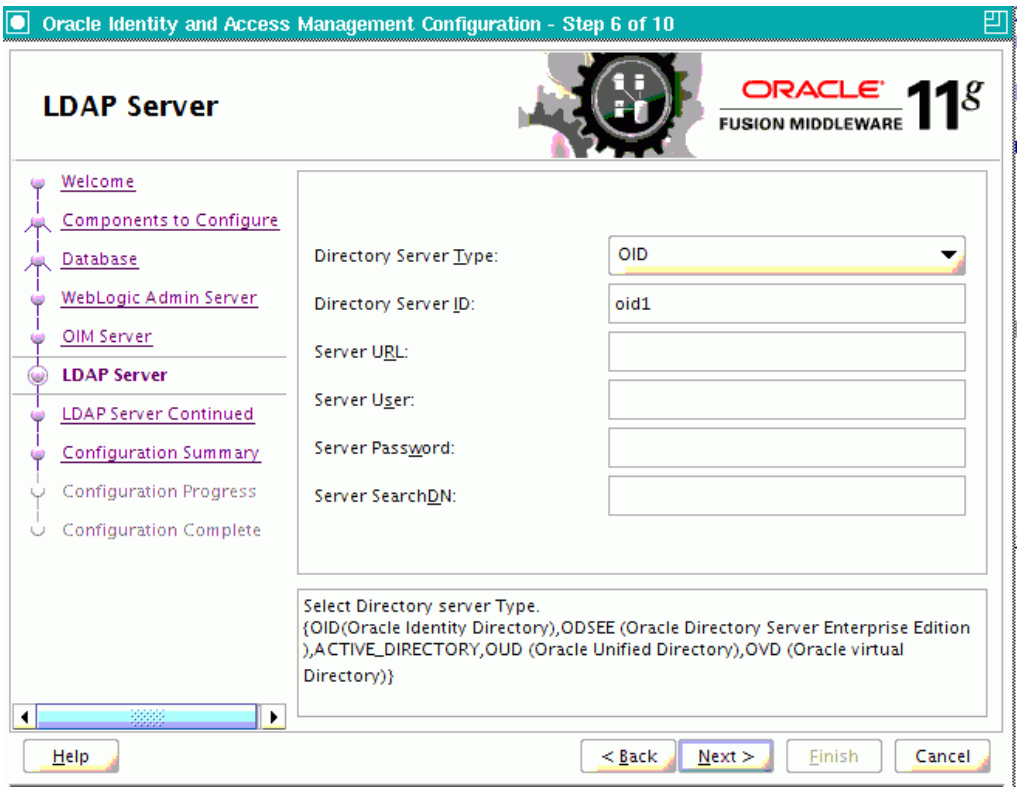


Table B–4 describes the parameters that you must specify.

Table B–4 LDAP Server Information

Field Name	Description
Directory Server Type	Select the desired Directory Server from the dropdown list.
Directory Server ID	Enter the Directory Server ID.
Server URL	Enter the LDAP URL in the format: `ldap://oid_host:oid_port`
Server User	Enter the user name for the Directory Server administrator. For example: `cn=oimAdminUser,cn=Users,dc=mycompany,dc=com`
Server Password	Enter the OIM admin password
Server 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.

B.7 LDAP Server Continued

This screen is a continuation of the LDAP Server screen.

Figure B–7 LDAP Server Continued Screen

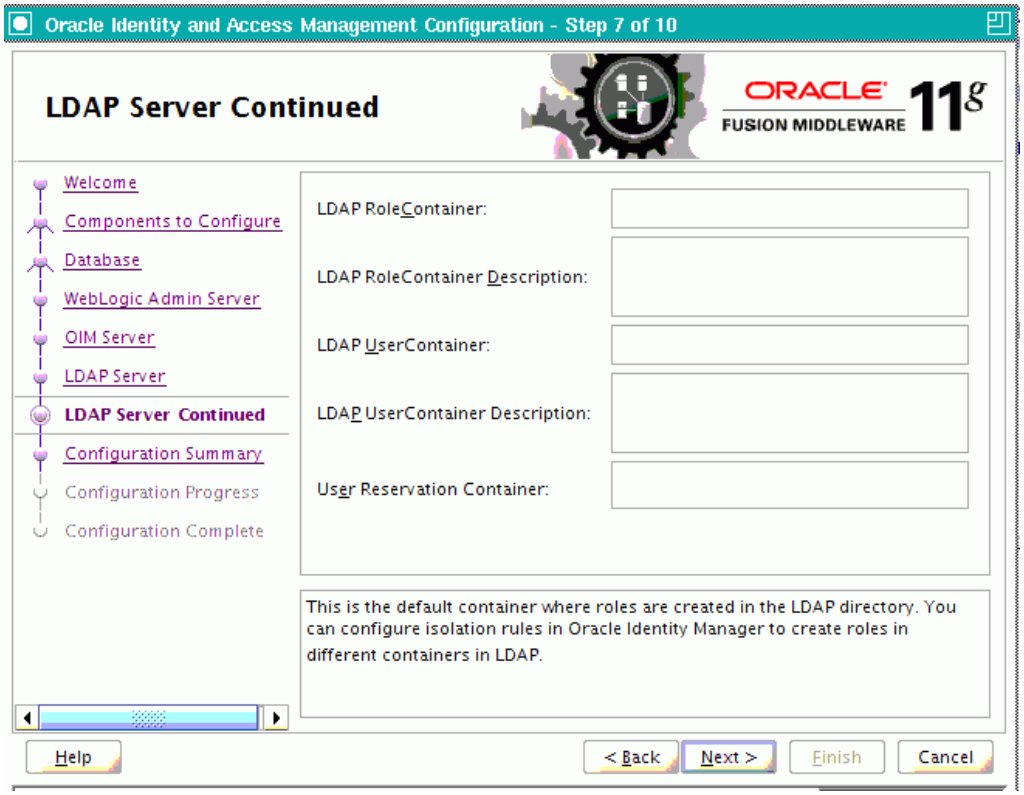


Table B–5 describes the LDAP parameters that you must specify.

Table B–5 LDAP Server Continued Information

Field Name	Description
LDAP RoleContainer	Enter a name for the container that will be used as a default container of roles in the LDAP directory.
LDAP RoleContainer Description	Type a description for the role container.
LDAP UserContainer	Enter a name for the container that will be used as a default container of users in the LDAP directory.
LDAP UserContainer Description	Type a description for the user container.
User Reservation Container	Enter a name for the container that will be used for reserving user names in the LDAP directory while their creation is being approved in Oracle Identity Manager. When the user names are approved, they are moved from the reservation container to the user container in the LDAP directory.

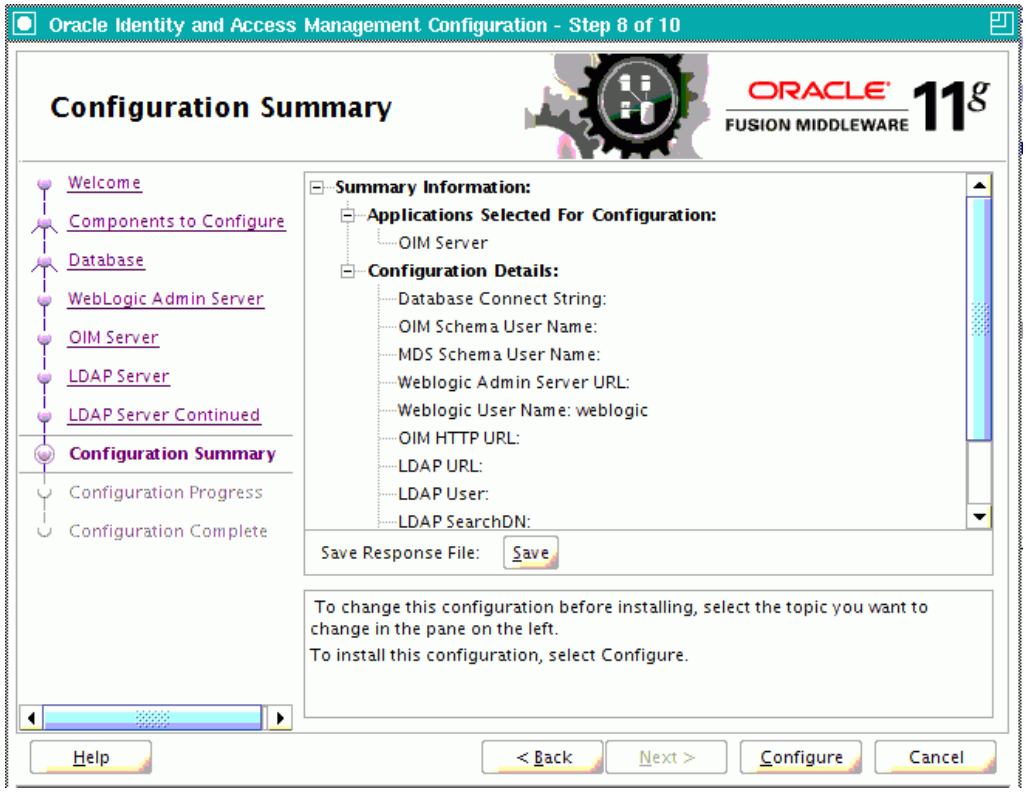
After entering information in the fields, click **Next** to continue.

B.8 Configuration Summary

This screen displays a list of the applications or components you have selected for configuration. It includes the following information:

- Location of your installation
- Disk space that will be used for the installation
- Applications or components you have selected for configuration
- Configuration choices you made on different screens in the Oracle Identity Manager Configuration Wizard

Figure B–8 Configuration Summary Screen



Review this summary screen.

Additionally, you can select to create a response file from your installation selections by clicking on the **Save** button in the Save Response File field. A response file can be used for silent or non-interactive installations of software requiring no or very little user input.

Click **Configure** to start configuring the selected Oracle Identity Manager components.

C

Starting or Stopping the Oracle Stack

You must start or stop the components of the Oracle stack in a specific order. Oracle Stack refers to Administration Server for the WebLogic Server domain, the system components that are managed by Oracle Process Manager and Notification Server, and the Managed Servers, which are controlled by Node Manager.

This appendix describes that order and contains the following topics:

- Starting the Stack
- Stopping the Stack
- Restarting Servers

Note: When executing the startManagedWebLogic and stopManagedWebLogic scripts described in the following topics:

- *SERVER_NAME* represents the name of the Oracle WebLogic Managed Server, such as `wls_oif1`, `wls_ods1`, or `oam_server1`.
- You will be prompted for values for *USER_NAME* and *PASSWORD* if you do not provide them as options when you execute the script.
- The value for *ADMIN_URL* will be inherited if you do not provide it as an option when you execute the script.

C.1 Starting the Stack

After completing the installation and domain configuration, you must start the Administration Server and various Managed Servers to get your deployments up and running:

1. To start the Administration Server, run the `startWebLogic.sh` (on UNIX operating systems) or `startWebLogic.cmd` (on Windows operating systems) script in the directory where you created your new domain.

   On UNIX systems:

   MW_HOME`/user_projects/domains/`*domain_name*`/startWebLogic.sh`

   On Windows systems:

   MW_HOME`\user_projects\domains\`*domain_name*`\startWebLogic.cmd`

domain_name is the name of the domain that you entered on the Specify Domain Name and Location Screen in the Oracle Fusion Middleware Configuration Wizard.

2. Configure Node Manager to start the Managed Servers. If a Managed Server contains other Oracle Fusion Middleware products, such as Oracle SOA Suite, Oracle WebCenter, or Oracle JRF, the Managed Servers environment must be configured to set the correct classpath and parameters. This environment information is provided through the start scripts, such as `startWebLogic` and `setDomainEnv`, which are located in the domain directory.

   If the Managed Servers are started by Node Manager (as is the case when the servers are started by the Oracle WebLogic Server Administration Console or Fusion Middleware Control), Node Manager must be instructed to use these start scripts so that the server environments are correctly configured. Specifically, Node Manager must be started with the property `StartScriptEnabled=true`.

   There are several ways to ensure that Node Manager starts with this property enabled. As a convenience, Oracle Fusion Middleware provides the following script, which adds the property `StartScriptEnabled=true` to the `nodemanager.properties` file:

   On UNIX:

   1. Run the following script to add the property `StartScriptEnabled=true` to the `nodemanager.properties` file:

      ORACLE_COMMON_HOME`/common/bin/setNMProps.sh`

   2. Start the Node Manager by executing the following command:

      MW_HOME`/WLS_HOME/server/bin/startNodeManager.sh`

   On Windows:

   1. Run the following script to add the property `StartScriptEnabled=true` to the `nodemanager.properties` file:

      ORACLE_COMMON_HOME`\common\bin\setNMProps.cmd`

   2. Start the Node Manager by executing the following command:

      MW_HOME`\WLS_HOME\server\bin\startNodeManager.cmd`

   Note: When you start Node Manager, it reads the `nodemanager.properties` file with the `StartScriptEnabled=true` property, and uses the start scripts when it subsequently starts Managed Servers. Note that you need to run the `setNMProps` script only once.

3. 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.

   Note: If the Node Manager is not running, you can 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 Management Server)
- `oim_server1` (Oracle Identity Manager Server)

For example, to start Oracle Access Management 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
-Dweblogic.system.StoreBootIdentity=true
```

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
-Dweblogic.system.StoreBootIdentity=true
```

Note: You can use the Oracle WebLogic Administration Console to start managed components in the background. See *Oracle Fusion Middleware Introduction to Oracle WebLogic Server* for more information.

If you do not know the names of the Managed Servers that should be started, you can view the contents of the following file on UNIX systems:

```
MW_HOME/user_projects/domains/domain_name/startManagedWebLogic_readme.txt
```

On Windows systems:

```
MW_HOME\user_projects\domains\domain_name\startManagedWebLogic_readme.txt
```

Or, you can access the Administration Server console at the following URL:

```
http://host:admin_server_port/console
```

Supply the user name and password that you specified on the Configure Administrator Username and Password Screen of the Configuration Wizard. Then, navigate to **Environment > Servers** to see the names of your Managed Servers.

C.2 Stopping the Stack

You can stop the Oracle WebLogic Administration Server and all the managed servers by using Oracle WebLogic Administration Console. See *Oracle Fusion Middleware Introduction to Oracle WebLogic Server* for more information.

To stop the stack components from the command line, perform the following steps:

1. Stop WebLogic managed components, such as Oracle Access Management, 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 the Oracle WebLogic Administration Server by executing the following command:

   ```
   MW_HOME/user_projects/domains/DOMAIN_NAME/bin/stopWebLogic.sh
   ```

3. If you want to stop the Node Manager, you can use the `kill` command:

   ```
   kill -9 PID
   ```

C.3 Restarting Servers

To restart the Administration Server or Managed Servers, you must stop the running Administration Server or Managed Servers first before starting them again. For more information, see Stopping the Stack and Starting the Stack.

D

Preconfiguring Oracle Directory Server Enterprise Edition (ODSEE)

Before you can use your LDAP directory as an Identity store, you must preconfigure it. The procedure in this section enables you to preconfigure Oracle Directory Server Enterprise Edition (ODSEE) for using Oracle Directory Server Enterprise Edition (ODSEE) as your LDAP Identity store.

Notes:

- If your LDAP Identity store (Oracle Directory Server Enterprise Edition (ODSEE) or iPlanet) has been configured for the containers and oimadminuser with the schema extension, you need not follow the below mentioned configuration steps.
- The data used in the examples provided below is a sample data. Follow the examples and replace them with appropriate data as per your LDAP server configuration.
- `cn=oracleAccounts` is a sample data. It is not mandatory to use this data when you preconfigure the Identity Store.

You must complete the following steps to preconfigure the Identity Store:

1. Create a new file `iPlanetContainers.ldif`. Add the following entries and save the file.

```
dn:cn=oracleAccounts,dc=mycompany,dc=com
cn:oracleAccounts
objectClass:nsContainer

dn:cn=Users,cn=oracleAccounts,dc=mycompany,dc=com
cn:Users
objectClass:nsContainer

dn:cn=Groups,cn=oracleAccounts,dc=mycompany,dc=com
cn:Groups
objectClass:nsContainer

dn:cn=Reserve,cn=oracleAccounts,dc=mycompany,dc=com
cn:Reserve
objectClass:nsContainer
```

2. Import the containers into iPlanet Directory Server with `ldapadd` command. This will create the user, group and reserve containers.

```
ldapadd -h <ODSEE Server> -p <ODSEE port> -D <ODSEE Admin ID> -w <ODSEE Admin
password> -c -f ./iPlanetContainers.ldif
```

For example:

```
ldapadd -h localhost -p 1389 -D "cn=Directory Manager" -w "welcome1" -c -f
./iPlanetContainers.ldif
```

If the above gives authentication error, try the command with '-x' option with simple bind option.

```
ldapadd -h localhost -p 1389 -x -D "cn=Directory Manager" -w "welcome1" -c -f
./iPlanetContainers.ldif
```

3. Enable the `moddn` property for the rename of entries to happen between nodes.

```
..dsee7/bin/dsconf set-server-prop -h <ODSEE Server> -p <ODSEE port>
moddn-enabled:on
```

For example:

```
..dsee7/bin/dsconf set-server-prop -h localhost -p 1389 moddn-enabled:on
```

4. Enable changelog.

```
..dsee7/bin/dsconf set-server-prop -h <ODSEE Server> -p <ODSEE port>
retro-cl-enabled:on
```

For example:

```
..dsee7/bin/dsconf set-server-prop -h localhost -p 1389 retro-cl-enabled:on
```

5. Check the status.

```
..dsee7/bin/dsccsetup status
```

6. Stop and Start the ODSEE server instance.

```
..dsee7/bin/dsadm stop <ODSEE instance>
..dsee7/bin/dsadm start <ODSEE instance>
```

For example:

```
..dsee7/bin/dsadm stop /scratch/<userid>/iPlanet/dsinst1/
..dsee7/bin/dsadm start /scratch/<userid>/iPlanet/dsinst1/
```

7. Extend the Sun schema to include OIM-specific Object Classes and Attribute Types.

```
cd to $MIDDLEWARE_HOME/oracle_common/modules/oracle.ovd_11.1.1/oimtemplates
```

Run the following command to load the ldif file, `sunOneSchema.ldif`.

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

For example:

```
./ldapmodify -h localhost -p 1389 -D "cn=directory manager" -w welcome1 -c -f
sunOneSchema.ldif
```

8. Enable Referential Integrity for OIM's Common Name Generation feature.

Anytime the DN or RDN is being modified, then the Referential Integrity needs to be enabled in OIM and OID/Active Directory/ODSEE.

If Referential Integrity is enabled in the Directory Server, then customers need to set the OIM property `XL.IsReferentialIntegrityEnabledInLDAP` to `TRUE` as by default it is set to `FALSE`. To set `XL.IsReferentialIntegrityEnabledInLDAP` to `TRUE`, log into OIM and go to **Advanced** > **System Management** > **System Configuration**. Search for System Properties (`XL.IsReferentialIntegrityEnabled`), and set the property value to `TRUE`.

a. Use the following command to see the value of the referential integrity property.

```
..dsee7/bin/dsconf get-server-prop -h <ODSEE server> -p <ODSEE port>
ref-integrity-enabled
Enter "cn=Directory Manager" password:
ref-integrity-enabled : off
```

b. Use the following commands to enable the referential integrity property.

```
./dsconf set-server-prop -h <ODSEE server> -p <ODSEE port>
ref-integrity-enabled:on
Enter "cn=Directory Manager" password:
```

Directory Server must be restarted for changes to take effect. Restart ODSEE/iPlanet Server after enabling referential integrity property.

```
..dsee7/bin/dsadm stop <ODSEE instance>
..dsee7/bin/dsadm start <ODSEE instance>
```

For Example:

```
..dsee7/bin/dsadm stop /scratch/<userid>/iPlanet/dsinst1/
..dsee7/bin/dsadm start /scratch/<userid>/iPlanet/dsinst1/
```

c. Now query to see if the value has been set correctly.

```
..dsee7/bin/dsconf get-server-prop -h <ODSEE server> -p <ODSEE port>
ref-integrity-enabled
Enter "cn=Directory Manager" password:
ref-integrity-enabled : on
```

9. Create the OIM Admin User, Group and the ACIs. Open a new file `oimadminuser.ldif`. This oimadminuser would be used as a proxy user for OIM.

The root suffix is given as `dc=mycompany,dc=com`. This can be replaced with the appropriate root suffix of the ODSEE server.

a. Add the following LDAP entries and save the file `oimadminuser.ldif`. Run the following command to load the ldif file, `oimadminuser.ldif`.

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

dn: cn=systemids,dc=mycompany,dc=com
changetype: add
objectclass: nsContainer
objectclass: top
cn: systemids

dn: cn=oimAdminUser,cn=systemids,dc=mycompany,dc=com
changetype: add
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetorgperson
```

```
mail: oimAdminUser
givenname: oimAdminUser
sn: oimAdminUser
cn: oimAdminUser
uid: oimAdminUser
userPassword: welcome1

dn: cn=oimAdminGroup,cn=systemids,dc=mycompany,dc=com
changetype: add
objectclass: groupOfUniqueNames
objectclass: top
cn: oimAdminGroup
description: OIM administrator role
uniquemember: cn=oimAdminUser,cn=systemids,dc=mycompany,dc=com

dn: cn=users,cn=oracleAccounts,dc=mycompany,dc=com
changetype: modify
add: aci
aci: (target =
"ldap:///cn=users,cn=oracleAccounts,dc=mycompany,dc=com")(targetattr =
 "*")(version 3.0; acl "Allow OIMAdminGroup add, read and write access to
 all attributes"; allow (add, read, search, compare,write, delete, import)
 (groupdn = "ldap:///cn=oimAdminGroup,cn=systemids,dc=mycompany,dc=com");)

dn: cn=Groups,cn=oracleAccounts,dc=mycompany,dc=com
changetype: modify
add: aci
aci: (target =
"ldap:///cn=Groups,cn=oracleAccounts,dc=mycompany,dc=com")(targetattr =
 "*")(version 3.0; acl "Allow OIM AdminGroup to read and write access";
 allow (read, search, compare, add, write,delete) (groupdn =
 "ldap:///cn=oimAdminGroup,cn=systemids,dc=mycompany,dc=com");)

dn: cn=reserve,cn=oracleAccounts,dc=mycompany,dc=com
changetype: modify
add: aci
aci: (target =
"ldap:///cn=reserve,cn=oracleAccounts,dc=mycompany,dc=com")(targetattr =
 "*")(version 3.0; acl "Allow OIM AdminGroup to read and write access";
 allow (read, search, compare, add, write,delete,export) (groupdn =
 "ldap:///cn=oimAdminGroup,cn=systemids,dc=mycompany,dc=com");)

dn: cn=changelog
changetype: modify
add: aci
aci: (target = "ldap:///cn=changelog")(targetattr = "*")(version 3.0; acl
 "Allow OIM AdminGroup to read and write access"; allow (read, search,
 compare, add, write,delete,export) (groupdn =
 "ldap:///cn=oimAdminGroup,cn=systemids,dc=mycompany,dc=com");)
```

b. Use the following commands to check for the entries and ACI in the LDAP:

```
ldapsearch -h <ODSEE Server> -p <ODSEE Port> -x -D "cn=Directory Manager"
 -w <ODSEE Admin Password> -b "cn=changelog" -s sub "objectclass=*" aci

ldapsearch -h <ODSEE Server> -p <ODSEE Port> -x -D "cn=Directory Manager"
 -w <ODSEE Admin Password> -b
"cn=users,cn=oracleAccounts,dc=mycompany,dc=com" -s sub
 "objectclass=*" aci

ldapsearch -h <ODSEE Server> -p <ODSEE Port> -x -D "cn=Directory Manager"
```

```
 -w <ODSEE Admin Password> -b
"cn=groups,cn=oracleAccounts,dc=mycompany,dc=com" -s sub
 "objectclass=*" aci
ldapsearch -h <ODSEE Server> -p <ODSEE Port> -x -D "cn=Directory Manager"
 -w <ODSEE Admin Password> -b
"cn=reserve,cn=oracleAccounts,dc=mycompany,dc=com" -s sub
 "objectclass=*" aci
```

E

Preconfiguring Oracle Unified Directory (OUD)

Before you can use your LDAP directory as an Identity store, you must preconfigure it. The procedure in this section enables you to preconfigure Oracle Unified Directory (OUD) for using Oracle Unified Directory (OUD) as your LDAP Identity store.

Notes:

- If your LDAP Identity store (Oracle Unified Directory (OUD)) has been configured for the containers and oimadminuser with the schema extension, you need not follow the below mentioned configuration steps.
- The data used in the examples provided below is a sample data. Follow the examples and replace them with appropriate data as per your LDAP server configuration.
- `cn=oracleAccounts` is a sample data. It is not mandatory to use this data when you preconfigure the Identity Store.

You must complete the following steps to preconfigure the Identity Store:

1. Create a new file `OUDContainers.ldif`. Add the following entries and save the file.

```
dn:cn=oracleAccounts,dc=mycompany,dc=com
cn:oracleAccounts
objectClass:top
objectClass:orclContainer

dn:cn=Users,cn=oracleAccounts,dc=mycompany,dc=com
cn:Users
objectClass:top
objectClass:orclContainer

dn:cn=Groups,cn=oracleAccounts,dc=mycompany,dc=com
cn:Groups
objectClass:top
objectClass:orclContainer

dn:cn=Reserve,cn=oracleAccounts,dc=mycompany,dc=com
cn:Reserve
objectClass:top
objectClass:orclContainer
```

2. Import the containers into Oracle Unified Directory Server with `ldapadd` command. This will create the user, group and reserve containers.

```
ldapadd -h <OUD Server> -p <OUD port> -D <OUD Admin ID> -w <OUD Admin password>
-c -f ./OUDContainers.ldif

For example:
ldapadd -h localhost -p 3389 -D "cn=Directory Manager" -w "welcome1" -c -f
./OUDContainers.ldif
```

If the above gives authentication error, try the command with '-x' option with simple bind option.

```
ldapadd -h localhost -p 1389 -x -D "cn=Directory Manager" -w "welcome1" -c -f
./OUDContainers.ldif
```

3. Configure OIM proxy users and acis to communicate with OUD after installing OUD. Create the OIM Admin User, Group and the ACIs.

   The root suffix is given as `dc=mycompany,dc=com`. This can be replaced with the appropriate root suffix of the OUD server.

   a. Open a new file `oudadmin.ldif`. Add the following LDAP entries and save the file `oudadmin.ldif`. Run the following command to load the ldif file, `oudadmin.ldif`.

Note: Run the `ldapmodify` command in OUD setup to add the OIM proxy User, OIM proxy Group and the relevant ACIs.

- The OIMAdmin proxy user must have the ACI allowing to write/reset the userPassword.
- The OIMAdmin proxy user must have the `password-reset` privilege. The `password-reset` privilege is assigned with a ldapmodify on the user entry.

```
cd <OUD instance>/bin

./ldapmodify -h <OUD Server> -p <OUD port> -D <OUD Admin ID> -j <pwd.txt>
-c-v-f oudadmin.ldif
Note: In the above command pwd.txt is the text file containing the OUD
Admin password.

dn: cn=systemids,dc=mycompany,dc=com
changetype: add
objectclass: orclContainer
objectclass: top
cn: systemids

dn: cn=oimAdminUser,cn=systemids,dc=mycompany,dc=com
changetype: add
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetorgperson
mail: oimAdminUser
givenname: oimAdminUser
sn: oimAdminUser
cn: oimAdminUser
uid: oimAdminUser
userPassword: welcome1
```

```
dn: cn=oimAdminGroup,cn=systemids,dc=mycompany,dc=com
changetype: add
objectclass: groupOfUniqueNames
objectclass: top
cn: oimAdminGroup
description: OIM administrator role
uniquemember: cn=oimAdminUser,cn=systemids,dc=mycompany,dc=com

dn: cn=oracleAccounts,dc=mycompany,dc=com
changetype: modify
add: aci
aci: (target = "ldap:///cn=oracleAccounts,dc=mycompany,dc=com")(targetattr
=
 "*")(version 3.0; acl "Allow OIMAdminGroup add, read and write access to
 all attributes"; allow (add, read, search, compare,write, delete,
import,export)
 (groupdn = "ldap:///cn=oimAdminGroup,cn=systemids,dc=mycompany,dc=com");)

dn: cn=oimAdminUser,cn=systemids,dc=mycompany,dc=com
changetype: modify
add: ds-privilege-name
ds-privilege-name: password-reset
```

b. Perform the following steps to configure the changelog on OUD server:

Note: Perform these steps only if the replication has not been configured during the installation of OUD server.

Create a replication server using `dsconfig` command:

```
dsconfig -h <OUD host> -p <OUD Admin SSL Port> -D <OUD Admin id> -j
 <password file> -X -n create-replication-server --provider-name
 'Multimaster Synchronization' --set replication-port:8989 --set
 replication-server-id:1 --type generic
```

Create a replication domain using `dsconfig` command:

```
dsconfig -h <OUD host> -p <OUD Admin SSL port> -D <OUD Admin id> -j
 <password file> -X -n create-replication-domain --provider-name
 'Multimaster Synchronization' --set base-dn:<dc=myDomain,dc=com> --set
replication-server:<OUD host>:8989 --set server-id:1 --type generic
--domain-name <dc=myDomain,dc=com>
```

c. Use the following command to check if the ACI is added.

```
./ldapsearch -h <OUD Server> -p <OUD Port> -D "cn=Directory Manager"
 -j <pwd.txt> -b "dc=mycompany,dc=com" -s base "objectclass=*" aci
Note: In the above command pwd.txt is the text file containing the OUD
Admin password.
```

d. Use the following command to check if the proxy user is working against OUD.

```
./ldapsearch -h <OUD Server> -p <OUD Port> -D
 "cn=oimAdminUser,cn=systemids,dc=oracle,dc=com" -j <pwd.txt> -b
 "cn=changelog" -s sub "changenumber>=0"
Note: In the above command pwd.txt is the text file containing the OUD
Admin password.
```

4. Complete the following steps for the access controls in OUD (ACI):

   Add the global-aci to changelog node in OUD.

   Refer to the "Using dsconfig in Interactive Mode" topic in the *Oracle Fusion Middleware Administrator's Guide for Oracle Unified Directory* 11*g* Release 2 (11.1.2) available at the following link:

   http://docs.oracle.com/cd/E29407_01/admin.111200/e22648/server_config.htm#solUSING-DSCONFIG-IN-INTERACTIVE-MODE

   Follow the steps in the document mentioned above and add the global-aci to `cn=changelog` entry in OUD:

   ```
   (target="ldap:///cn=changelog")(targetattr="*")(version 3.0; acl "External
   changelog access"; allow(read,search,compare,add,write,delete,export)
   groupdn="ldap:///cn=oimAdminGroup,cn=systemids,dc=mycompany,dc=com";)

   dn: cn=Reserve,dc=mycompany,dc=com
   changetype: modify
   add: aci
   aci: (target="ldap:///cn=Reserve,dc=mycompany,dc=com")(targetattr="*")(version
   3.0; acl "Allow OIMAdminGroup add, read and write access to all attributes";
   allow (add, read, search, compare,write, delete, import,export)(groupdn =
   "ldap:///cn=oimAdminGroup,cn=Groups,dc=mycompany,dc=com");)
   ```

   You must remove `deny` from this global-aci and `allow` the oim proxy user, otherwise `deny` will take priority.

   Note: If you are using OUD 11.1.1.5.0, use the following ACI:

   ```
   (target="ldap:///cn=changelog")(targetattr="*")(version 3.0; acl
    "External changelog access";deny (all)
   groupdn!="ldap:///cn=oimAdminGroup,cn=systemids,dc=myDomain,dc=com"
   ;)
   ```

   Refer to the *Oracle Fusion Middleware Administrator's Guide for Oracle Unified Directory* 11*g* Release 2 (11.1.2) available at the following link:

   http://docs.oracle.com/cd/E29407_01/admin.111200/e22648/server_config.htm#solUSING-DSCONFIG-IN-INTERACTIVE-MODE

   Follow the steps in the document mentioned above and delete the default `deny` global-aci from `cn=changelog` entry in OUD.

   ```
   (target="ldap:///cn=changelog")(targetattr="*")(version 3.0; acl
   "External changelog access"; deny (all) userdn="ldap:///anyone";)
   ```

5. If you want to enable Oracle Identity Manager (OIM) to lock a user account, you must configure a password policy on OUD server.

   In the password policy, you must define the maximum number of failed logins the source LDAP directory server requires, to lock the account. This max number must have the same value as defined in the User Management plugin (`pwdMaxFailure` parameter) in Section 5.9.5.2.4, "Creating Adapters for Oracle Unified Directory (OUD)".

   Use the following command to configure OUD password policy (for instance 3 failures locks the account):

   ```
   dsconfig -h <OUD host> -p <OUD Admin SSL port> -D <OUD Admin id> -j <password
   file> -X -n set-password-policy-prop --policy-name 'Default Password Policy'
   ```

```
--set lockout-failure-count:3
```

F

Preconfiguring Oracle Internet Directory (OID)

Before you can use your LDAP directory as an Identity store, you must preconfigure it. The procedure in this section enables you to preconfigure Oracle Internet Directory (OID) for using Oracle Internet Directory (OID) as your LDAP Identity store.

Notes:

- If your LDAP Identity store (Oracle Internet Directory (OID)) has been configured for the containers and oimadminuser with the schema extension, you need not follow the below mentioned configuration steps.
- The data used in the examples provided below is a sample data. Follow the examples and replace them with appropriate data as per your LDAP server configuration.
- `cn=oracleAccounts` is a sample data. It is not mandatory to use this data when you preconfigure the Identity Store.

You must complete the following steps to preconfigure the Identity Store:

1. Create a new file `OIDContainers.ldif`. Add the following entries and save the file.

```
dn:cn=oracleAccounts,dc=mycompany,dc=com
cn:oracleAccounts
objectClass:top
objectClass:orclContainer

dn:cn=Users,cn=oracleAccounts,dc=mycompany,dc=com
cn:Users
objectClass:top
objectClass:orclContainer

dn:cn=Groups,cn=oracleAccounts,dc=mycompany,dc=com
cn:Groups
objectClass:top
objectClass:orclContainer

dn:cn=Reserve,cn=oracleAccounts,dc=mycompany,dc=com
cn:Reserve
objectClass:top
objectClass:orclContainer
```

2. Import the containers into Oracle Internet Directory Server with `ldapadd` command. This will create the user, group and reserve containers.

```
ldapadd -h <OID Server> -p <OID port> -D <OID Admin ID> -w <OID Admin password>
-c -f ./OIDContainers.ldif

For example:
ldapadd -h localhost -p 3060 -D "cn=orcladmin" -w "welcome1" -c -f
./OIDContainers.ldif
```

If the above gives authentication error, try the command with '-x' option with simple bind option.

```
ldapadd -h localhost -p 3060 -x -D "cn=orcladmin" -w "welcome1" -c -f
./OIDContainers.ldif
```

3. Configure OIM proxy users and acis to communicate with OID after installing OID. Create the OIM Admin User, Group and the ACIs.

The root suffix is given as 'dc=mycompany,dc=com'. This can be replaced with the appropriate root suffix of the OID server.

a. Open a new file `oidadmin.ldif`. Add the following LDAP entries and save the file `oidadmin.ldif`. Run the following command to load the ldif file, `oidadmin.ldif`.

Note: Run the `ldapmodify` command in OID setup to add the OIM proxy User, OIM proxy Group and the relevant ACIs.

```
./ldapmodify -h <OID Server> -p <OID port> -D <OID Admin ID> -w <OID Admin
password> -c-v-f oidadmin.ldif

dn: cn=systemids,dc=mycompany,dc=com
changetype: add
objectclass: orclContainer
objectclass: top
cn: systemids

dn: cn=oimAdminUser,cn=systemids,dc=mycompany,dc=com
changetype: add
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetorgperson
objectclass: orcluser
objectclass: orcluserV2
mail: oimAdminUser
givenname: oimAdminUser
sn: oimAdminUser
cn: oimAdminUser
uid: oimAdminUser
userPassword: welcome1

dn: cn=oimAdminGroup,cn=systemids,dc=mycompany,dc=com
changetype: add
objectclass: groupOfUniqueNames
objectclass: orclPrivilegeGroup
objectclass: top
cn: oimAdminGroup
```

```
description: OIM administrator role
uniquemember: cn=oimAdminUser,cn=systemids,dc=mycompany,dc=com

dn: cn=oracleAccounts,dc=mycompany,dc=com
changetype: modify
add: orclaci
orclaci: access to entry by
group="cn=oimAdminGroup,cn=systemids,dc=mycompany,dc=com"
(add,browse,delete) by * (none)
orclaci: access to attr=(*) by
group="cn=oimAdminGroup,cn=systemids,dc=mycompany,dc=com"
(read,search,write,compare) by * (none)

dn: cn=changelog
changetype: modify
add: orclaci
orclaci: access to entry by
group="cn=oimAdminGroup,cn=systemids,dc=mycompany,dc=com" (browse) by *
(none)
orclaci: access to attr=(*) by
group="cn=oimAdminGroup,cn=systemids,dc=mycompany,dc=com"
(read,search,compare) by * (none)
```

b. Use the following command to check if the ACI is added.

```
./ldapsearch -h <OID Server> -p <OID Port> -D "cn=orcladmin"
 -w <OID Admin password> -b "dc=mycompany,dc=com" -s one "objectclass=*"
orclaci
```

c. Use the following command to check if the proxy user is working against OID. Before running this command ensure that the `changenumber` is catalogued.

```
./ldapsearch -h <OID Server> -p <OID Port> -D
 "cn=oimAdminUser,cn=systemids,dc=mycompany,dc=com" -w <OID Admin password>
-b
 "cn=changelog" -s sub "changenumber>=0"
```

If the above command gives an error, try the following:

```
./ldapsearch -h <OID Server> -p <OID Port> -D
 "cn=oimAdminUser,cn=systemids,dc=mycompany,dc=com" -w <OID Admin password>
-b
 "cn=changelog" -s one "changenumber>=0"
```

G

Preconfiguring Active Directory

Before you can use your LDAP directory as an Identity store, you must preconfigure it. The procedure in this section enables you to preconfigure Microsoft Active Directory for using it as your LDAP Identity store.

You must complete the following steps to preconfigure the Identity Store:

> **Note:** The data used in the examples provided below is a sample data. Follow the examples and replace them with appropriate data as per your LDAP server configuration.

1. Create Reserve Container.

   ```
   dn:cn=Reserve,dc=extranetdev,dc=lan
   cn:Reserve
   objectClass:top
   ```

2. Create user for OIM - **uid: oimadmin pw:welcome11gR2** -in the Directory Server outside the search base used for OIM reconciliation.
3. Create user - **uid: xelsysadm pw:welcome11gR2**
4. Create a group **OIM Administrators** and assign the users **oimadmin and xelsysadm** users to the group
5. If you want to enable OAM-OIM integration, then create user for OAM - **uid:oamadmin pw:welcome11gR2**
6. If you want to enable OAM-OIM integration, then create a group **OAM Administrators** and assign the **oamadmin** user to the group
7. If you want to enable OAM-OIM integration, then create user for WebLogic Administration - **uid:WLAdmin pw:welcome11gR2**
8. If you want to enable OAM-OIM integration, then create a group **WLSAdmins** and assign the **oamadmin** user to the group
9. Add the ACLs that needs to be setup:

   OIM Administrators group - complete read/write privileges to all the user and group entities in the directory. This group needs **read/write privileges** for the **Reserve container** also.

10. Extend the OIM Schema for Active Directory.

    The OIM Schema for Active Directory is located at:

    MW_HOME/oracle_common/modules/oracle.ovd_11.1.1/oimtemplates

The following LDIF files are located at the *IAM_HOME*/oam/server/oim-intg/ldif/ad/schema directory:

- adOAMDisable.ldif
- adOAMEnable.ldif
- adOIMLanguageSubtype.ldif
- adOIMSchema.ldif

Run the following command to extend Active Directory schema:

On Windows:

```
extendadschema.bat -h AD_host -p AD_port -D <administrator@mydomain.com> -AD
<dc=mydomain,dc=com> -OAM <true/false>
```

On UNIX:

```
extendadschema.sh -h AD_host -p AD_port -D <administrator@mydomain.com> -AD
<dc=mydomain,dc=com> -OAM <true/false>
```

Specify the value of -OAM patameter as true if you want to enable OAM-OIM integration.

Specify the value of -OAM patameter as false if you do not want to enable OAM-OIM integration.

Note: The extendadschema script is certified only on Active Directory 2003, 2008 and 2008R2.

---

11. If you want to enable OAM-OIM integration, extend the OAM schema, as follows:

Navigate to the *IAM_HOME*/oam/server/oim-intg/ldif/ad/schema directory, and locate the following files:

- ADUserSchema.ldif
- AD_oam_pwd_schema_add.ldif

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

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

a. Navigate to thefollowing directory:

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

b. Run the ldapadd command.

```
ldapadd -h <activedirectoryhostname> -p <activedirectoryportnumber> -D <AD_
administrator> -q -c -f ADUserSchema.ldif

ldapadd -h <activedirectoryhostname> -p <activedirectoryportnumber> -D <AD_
administrator> -q -c -f AD_oam_pwd_schema.ldif
```

where *AD_administrator* is the user with schema extension privileges to the directory.

For example:

```
ldapadd -h activedirectoryhost.mycompany.com -p 389 -D adminuser -q -c -f
```

```
ADUserSchema.ldif
```

H

Creating Oracle Entitlement Server Schemas for Apache Derby

Apache Derby 10.5.3.0 is an evaluation database included in your Oracle WebLogic Server installation. If you are using Apache Derby for Oracle Entitlements Server policy store, you must create schemas for Oracle Entitlements Server as described in this appendix.

> **Note:** Derby policy store is supported only on WebLogic Server. Derby database should be used for development purposes only.
>
> Oracle strongly recommends you to use Oracle Database.

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

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

   ```
   DERBY_HOME="MW_HOME/wlserver_10.3/common/derby"
   ```

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

   - `setNetworkServerCP` (located in `MW_HOME/wlserver_10.3/common/derby/bin` on UNIX) or `setNetworkServerCP.bat` (located in `MW_HOME\wlserver_10.3\common\derby\bin` on Windows).
   - `startNetworkServer` (located in `MW_HOME/wlserver_10.3/common/derby/bin` on UNIX) or `startNetworkServer.bat` (located in `MW_HOME\wlserver_10.3\common\derby\bin` on Windows).

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

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

   ```
   bin/ij
   ```

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

```
ij> connect 'jdbc:derby://myhost/data/oesdb;create=true';
```

`oesdb` is the name of database and `data` is the relative path (based on the directory where you start the server. In this example, it is `Oracle/Middleware/wlserver_10.3/common/derby/bin` where the database files will be saved.

5. Open `opss_user.sql` (located in `RCU_HOME/rcu/integration/opss/scripts/derby`) in a text editor and replace `&&1` with the schema owner.

   Note: After you download the `rcuHome.zip` file, extract the contents of the `rcuHome.zip` file to a directory of your choice. This directory is referred to as the *RCU_HOME* directory.

   For more information about Repository Creation Utility (RCU), refer to the *Oracle Fusion Middleware Repository Creation Utility User's Guide*.

   Repeat the above steps for the following SQL files (located in `RCU_HOME/rcu/integration/opss/scripts/derby`):

   - `opss_tables.sql`
   - `opss_version.sql`
   - `opss_gencatalog.sql`

   Note: This is the schema owner that you will need to specify when you configure the Oracle Entitlements Server described in Configuring Oracle Entitlements Server Administration Server.

   Oracle Identity and Access Management components require the existence of schemas in a database prior to installation. These schemas are created and loaded in your database using the Repository Creation Utility (RCU).

6. Run the following SQL files (located in `RCU_HOME/rcu/integration/apm/sql/derby`) in the ij console:

   - `run'opss_user.sql';`
   - `run'opss_tables.sql';`
   - `run'opss_version.sql';`
   - `run'opss_gencatalog.sql';`

   Note: Ensure that you run the SQL files in the same order listed above and make a note of the schema owner and password that you have created.

Configuring the PDP Proxy Client for Web Service Security Module

This appendix provides a sample procedure for configuring the PDP Proxy Client for your Web Service Security Module.

Before you configuring the PDP Proxy Client for your Web Service Security Module, ensure that you have deployed a Web Service Security Module on a WebLogic Server domain. Your client application is another WebLogic Server deployed application. This client application needs to connect to the Web Service Security Module (PDP) for authorization decisions. You need to use a PDP proxy client to connect via a web service call to this Web Service Security Module (PDP). In this scenario, you create another WebLogic Server domain that is configured as a web service proxy Security Module. When the WebLogic Server domain application using this Security Module proxy instance makes OES PEP API calls, the proxy code manages making the associated web service calls to your web service domain for authorization decisions.

Complete the following steps to configure the PDP Proxy Client for your Web Service Security Module:

1. Configure properties in the `smconfig.prp` file by performing the following steps:
   a. Navigate to the SMConfigTool folder.

      ```
      $ cd $MW_HOME/oes_client/oessm/SMConfigTool
      ```

      Copy the originally backed up `smconfig.prp.bak` file to a new file, for example, `wls-wsproxy-smconfig.prp`.

      ```
      $ cp smconfig.prp.bak wls-wsproxy-smconfig.prp
      ```

   b. Open the `wls-wsproxy-smconfig.prp` file in your preferred editor and set the properties shown in Table I–1, leaving all other properties at their existing values.

Table I–1 Properties for the smconfig File

Property	Value
`oracle.security.jps.runtime.pd.client.policyDistributionMode`	non-controlled
`oracle.security.jps.pdp.isProxy`	True
`oracle.security.jps.pdp.PDPTransport`	WS

Table I–1 (Cont.) Properties for the smconfig File

Property	Value
`oracle.security.jps.pdp.proxy.PDPAddress`	`http://hostname:port` **Note:** The port number is the listening port of the WebLogic Server.

Save the `wls-wsproxy-smconfig.prp` file.

2. Navigate to the `$OES_CLIENT_HOME/oessm/bin` folder.

```
$ cd OES_CLIENT_HOME/oessm/bin
```

3. Perform the following steps to run the OES Configuration Wizard that creates the WLS WS proxy SM domain:

   a. Execute the SM config tool using the following command:

```
$ ./config.sh -smConfigId yourSMConfigID -smType wls
-serverLocation $MW_HOME/wlserver_10.3 -prpFileName
../SMConfigTool/wls-wsproxy-smconfig.prp
```

   b. The Fusion Middleware Configuration Wizard appears after you invoke the Security Module configuration tool.

   c. On the Welcome screen, select the **Create a new WebLogic domain** option. Click **Next**.

      The Select Domain Source screen appears.

   d. On the Select Domain Source screen, ensure that the **Generate a domain configured automatically to support the following products:** option is selected.

      Select the **Oracle Entitlements Server WebLogic Security Module- 11.1.1.0 [oesclient]** option. Click **Next**.

      Note: Ensure that you do not select the domain template **Oracle Entitlements Server for Admin Server - 11.1.1.0 [IAM_HOME]** which is associated with the Oracle Entitlements Server Administration Server.

      The Specify Domain Name and Location screen appears.

   e. Enter a name and a location for the domain to be created, and click **Next**.

      The Configure Administrator User Name and Password screen appears.

   f. Enter a user name and a password for the administrator. The default user name is `weblogic`. Click **Next**.

      The Configure Server Start Mode and JDK screen appears.

      Note: When you enter the user name and the password for the administrator, be sure to remember them.

      ---

   g. Choose a JDK from the **Available JDKs** and then select a **WebLogic Domain Startup Mode**. Click **Next**.

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

The Select Optional Configuration screen is displayed.

h. On the Select Optional Configuration screen, select **Administration Server**, and click **Next**.

i. Configure the following Administration Server parameters:

Name: Valid server names are a string of characters (alphabetic and numeric). The name must be unique in the domain. For example, `AdminServer`.

Listen address: From the drop-down list, select a value for the listen address. See Specifying the Listen Address for information about the available values.

Listen port—Enter a valid value for the listen port to be used for regular, nonsecure requests (through protocols such as HTTP and T3). The default value is the next available listen port. If you leave this field blank, the default value is used. For example, `7001`.

Note: Ensure that the value for the listen port is different from the listen port of the other Oracle Identity and Access Management components. For more information, see "Managing Ports" in the *Oracle Fusion Middleware Administrator's Guide*.

SSL enabled—Select this check box to enable the SSL listen port. By default, SSL is disabled for all new servers.

SSL listen port—Enter a valid value to be used for secure requests (through protocols such as HTTPS and T3S). The default value is the next available listen port. If you leave this field blank, the default value is used. For example, `7002`.

Note: After you specify the SSL listen port value, you must update the `oracle.security.jps.pd.clientPort` property in the `smconfig.wls.controlled.prp` file or `smconfig.prp` file with the SSL listen port value. You must then run the `smconfig` tool for Oracle WebLogic Server Security Module and set the Administration Server SSL port to the port specified in `oracle.security.jps.pd.clientPort`.

j. On the Configuration Summary screen, review the domain configuration, and click **Create** to create the WebLogic Server Web Service proxy SM enabled domain.

k. On successful domain creation you may review the folder structure and files of the Web Service Security Module instance on Oracle WebLogic Server. The `jps-config.xml` configuration file for the Web Service Security Module instance on Oracle WebLogic Server is located in `$DOMAIN_HOME/config/oeswlssmconfig/AdminServer`.

The `jps-config.xml` file contains the configuration used for proxying PEP API web service based requests to your Web Service Security Module deployed on the other WebLogic domain.

J

Deinstalling and Reinstalling Oracle Identity and Access Management

This appendix provides information about deinstalling and reinstalling Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0). It contains the following topics:

- Deinstalling Oracle Identity and Access Management
- Reinstalling Oracle Identity and Access Management

> **Note:** Always use the instructions provided in this appendix for removing the software. If you try to remove the software manually, you may experience problems when you try to reinstall the software. Following the procedures in this appendix ensures that the software is properly removed.

J.1 Deinstalling Oracle Identity and Access Management

This topic contains procedures for deinstalling Oracle Identity and Access Management. It contains the following sections:

- Deinstalling the Oracle Identity and Access Management Oracle Home
- Deinstalling the Oracle Common Home

J.1.1 Deinstalling the Oracle Identity and Access Management Oracle Home

The deinstaller attempts to remove the Oracle Home directory from which it was started. Before you choose to remove your Oracle Identity and Access Management Oracle Home directory, make sure that it is not in use by an existing domain and that you stop all running processes that use this Oracle Home.

Deinstalling Oracle Identity and Access Management will not remove any WebLogic domains that you have created—it only removes the software in the Oracle Identity and Access Management Oracle Home directory.

> **Note:** The oraInventory is required for removing instances and Oracle Home. For example, on UNIX it can be found in the following location:
>
> /etc/oraInst.loc

This section describes how to deinstall your Oracle Identity and Access Management Oracle Home using the graphical, screen-based deinstaller. However, you can also

perform a silent deinstallation using a response file. A deinstall response file template that you can customize for your deinstallation is included in the `Disk1/stage/Response` directory on UNIX, or in the `Disk1\stage\Response` directory on Windows.

Perform the following steps to deinstall your Oracle Identity and Access Management Oracle Home using the graphical, screen-based deinstaller:

1. Verify your Oracle Identity and Access Management Oracle Home is not in use by an existing domain.
2. Stop all processes that use the Oracle Identity and Access Management Oracle Home.
3. Open a command prompt and move (cd) into the *IAM_ORACLE_HOME*`/oui/bin directory` (UNIX) or the *IAM_HOME*`\oui\bin directory` (Windows).
4. Invoke the Deinstaller from command line using the `-deinstall` option. For example:

   On UNIX:

   ```
   ./runInstaller -deinstall
   ```

   On Windows:

   ```
   setup.exe -deinstall
   ```

   The Welcome screen appears.
5. Click **Next**.

   In the Deinstall Oracle Home screen, you can save a response file that contains the deinstallation settings before deinstalling. Click **Deinstall**. The Deinstall Progress screen appears. This screen shows the progress and status of the deinstallation.

   Click **Finish** after the deinstallation progresses to 100%. The Deinstallation Complete screen appears.
6. Click **Finish** on the Deinstallation Complete screen to exit the deinstaller.

J.1.2 Deinstalling the Oracle Common Home

The *ORACLE_COMMON_HOME* directory located in the *MW_HOME* directory contains the binary and library files required for Oracle Enterprise Manager Fusion Middleware Control and Oracle Java Required Files (JRF). Before you deinstall the *ORACLE_COMMON_HOME* directory, ensure that no other Oracle Fusion Middleware software, such as Oracle SOA Suite, depends on *ORACLE_COMMON_HOME*. You cannot deinstall the *ORACLE_COMMON_HOME* directory until all software that depends on it has been deinstalled.

Perform the following steps to deinstall the *ORACLE_COMMON_HOME* directory:

1. Stop all processes that use the *ORACLE_COMMON_HOME* directory. To know all the processes that are using ORACLE_COMMON_HOME directory use the following commands:

   On UNIX:

   ```
   ps-ef grep <oracle_common>
   ```

   On Windows:

Use the Windows Task Manager to identify the processes that use the ORACLE_COMMON_HOME directory.

2. Deinstall your Oracle Identity and Access Management Oracle Home by performing the steps in Deinstalling the Oracle Identity and Access Management Oracle Home.

3. Open a command prompt and move (cd) into the *ORACLE_COMMON_HOME*/oui/bin/ directory (on UNIX) or the *ORACLE_COMMON_HOME*\oui\bin\ directory (on Windows).

4. Invoke the Deinstaller from command line using the -deinstall option and the -jreLoc option, which identifies the location where Java Runtime Environment (JRE) is installed. For example:

   On UNIX:

   ```
   ./runInstaller -deinstall -jreLoc FULL_PATH_TO_JRE_DIRECTORY
   ```

   On Windows:

   ```
   setup.exe -deinstall -jreLoc FULL_PATH_TO_JRE_DIRECTORY
   ```

   The Welcome screen appears.

5. Click **Next**. The Select Deinstallation Type screen appears.

6. Select the **Deinstall Oracle Home** option at the top of the Select Deinstallation Type screen.

   Note: The path to the *ORACLE_COMMON_HOME* directory appears in the text describing the **Deinstall Oracle Home** option.

   Click **Next**. The Deinstall Oracle Home screen appears.

7. Confirm the correct *ORACLE_COMMON_HOME* directory is listed and click **Deinstall**.

   The Deinstallation Progress screen appears, along with a Warning dialog box prompting you to confirm that you want to deinstall the *ORACLE_COMMON_HOME* directory.

8. Click **Yes** on the Warning dialog box to confirm you want to remove the *ORACLE_COMMON_HOME* directory. The deinstallation begins.

9. Click **Finish** after the deinstallation progresses to 100%. The Deinstallation Complete screen appears.

10. Click **Finish** on the Deinstallation Complete screen to exit the deinstaller.

J.2 Reinstalling Oracle Identity and Access Management

Perform the following steps to reinstall Oracle Identity and Access Management:

1. Verify the directory you want to reinstall Oracle Identity and Access Management into, does not contain an existing Oracle Identity and Access Management instance. If it does, you must deinstall it before reinstalling. You cannot reinstall Oracle Identity and Access Management 11g Release1(11.1.1) in a directory that contains an existing Oracle Identity and Access Management instance.

2. Reinstall Oracle Identity and Access Management as if it was the first installation by performing the steps in the appropriate procedure in this guide.

K

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?

K.1 General Troubleshooting Tips

If you encounter an error during installation:

- Consult the Oracle Fusion Middleware 11*g* Release 2 (11.1.2.2.0). 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 Section 2.1, "Reviewing System Requirements and Certification" for more information.
- Verify your system meets the minimum system requirements. See Section 2.1, "Reviewing System Requirements and Certification" for more information.
- Verify you have satisfied the dependencies for the deployment you are attempting. Each deployment documented in this guide contains a "Dependencies" section.
- If you entered incorrect information on one of the installation screens, return to that screen by clicking **Back** until you see the screen.
- If an error occurred while the Installer is copying or linking files:
  1. Note the error and review the installation log files.
  2. Remove the failed installation. See Appendix J, "Deinstalling and Reinstalling Oracle Identity and Access Management" for more information.
  3. Correct the issue that caused the error.
  4. Restart the installation.
- If an error occurred while configuring Oracle Identity Manager using the Oracle Identity Manager Configuration Wizard:
  1. Note the error and review the configuration log files.

2. Verify whether the dependencies are met. For example, Administration Server and Database should be up and running.
3. Correct the issue that caused the error.
4. Restart the Oracle Identity Manager Configuration Wizard.

K.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

K.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 Appendix C.1, "Starting the Stack".

K.4 Need More Help?

If you cannot solve a problem using the information in this appendix, look for additional information in My Oracle Support at

`http://support.oracle.com`.

If you cannot find a solution to your problem, open a service request.

L

Oracle Adaptive Access Manager Partition Schema Reference

This appendix provides information about tables and stored procedures used with Oracle Adaptive Access Manager with Partition support.

It contains the following topics:

- Overview
- Partition Add Maintenance
- Partition Maintenance Scripts

L.1 Overview

Database tables in the Oracle Adaptive Access Manager database are divided into the following categories:

- Static partition tables
- Transactional partition tables
- Non-partitioned tables

> **Note:** All the tables contain the composite partition (RANGE, HASH). The Range partition is created using `CREATE_TIME` while the `HASH` key is defined based on application logic.
>
> Table L–1 lists the Oracle Adaptive Access Manager partition tables. All the other tables are non-partitioned.

Table L–1 Oracle Adaptive Access Manager 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

L.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

L.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.

L.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.

L.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 in <IAM_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.

L.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.

L.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.

L.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.

L.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.

M

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 and Access Management software from your machine. This appendix contains the following topics:

- Welcome
- Select Deinstallation Type
- Deinstallation Progress
- Deinstallation Complete

M.1 Welcome

The Welcome screen is the first screen that appears when you start the Oracle Fusion Middleware 11*g* Deinstallation Wizard.

Figure M–1 Welcome Screen

Click **Next** to continue.

M.2 Select Deinstallation Type

Select the type of deinstallation you want to perform.

Figure M–2 Select Deinstallation Type Screen

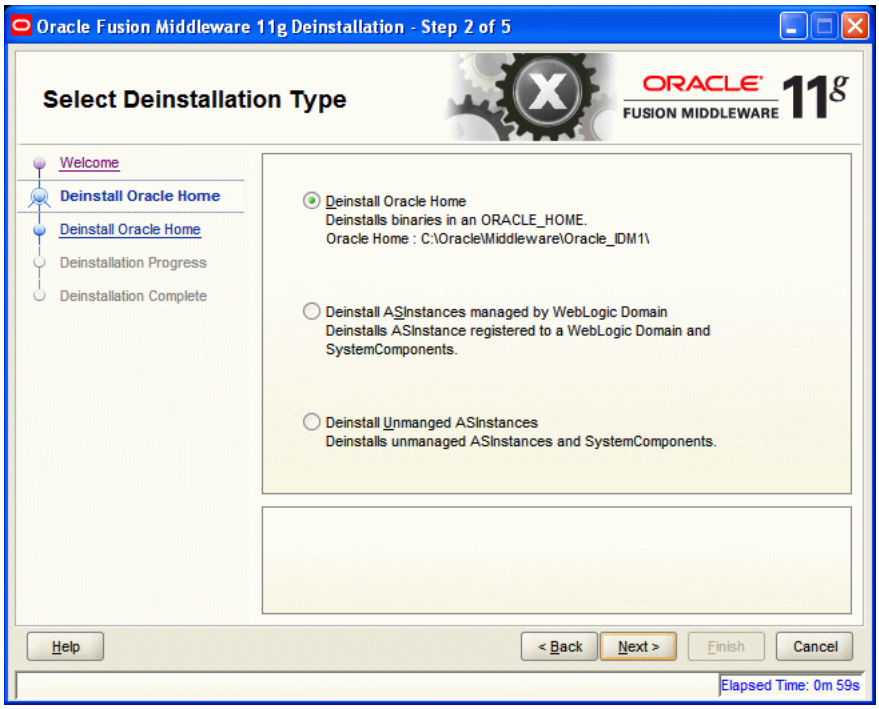


Table M–1 Deinstallation Types

Type	Description
Deinstall Oracle Home	Select this option to deinstall the binaries contained in the listed Oracle Identity and Access 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 and Access 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.

Click **Next** to continue.

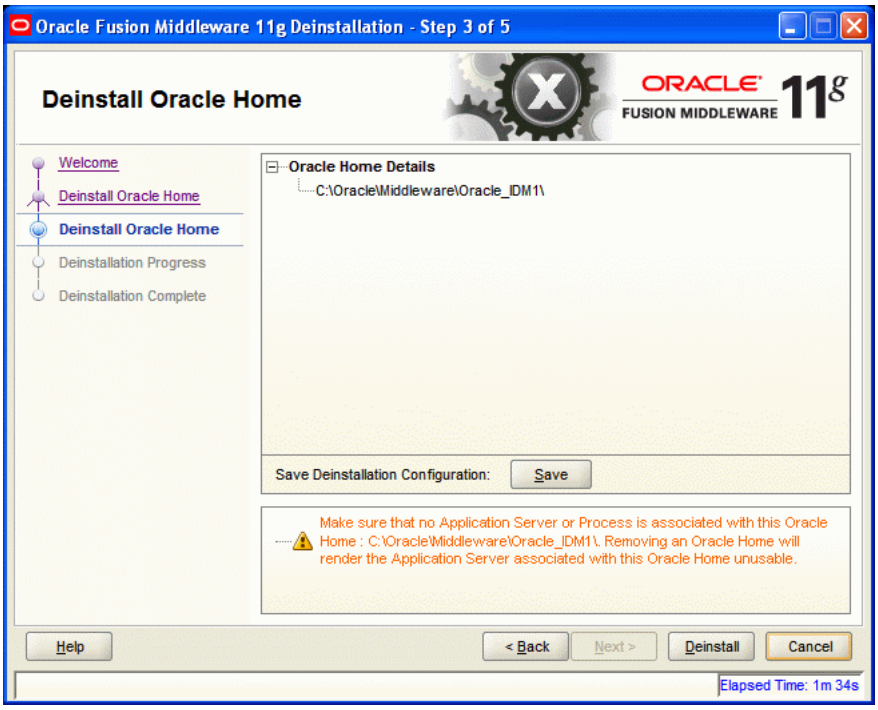
M.2.1 Option 1: Deinstall Oracle Home

If you selected **Deinstall Oracle Home** on the Select Deinstallation Type screen, the following screen appears:

M.2.1.1 Deinstall Oracle Home

This screen shows the Oracle Home directory that is about to be deinstalled. It is the Oracle Home directory in which the deinstaller was started.

Figure M–3 Deinstall Oracle Home Screen



Verify that this is the correct directory, and also verify that there are no processes associated with this Oracle Home.

Click **Deinstall** to start the deinstallation process.

M.2.2 Option 2: Deinstall ASInstances managed by WebLogic Domain

If you selected **Deinstall ASInstances managed by WebLogic Domain** on the Select Deinstallation Type screen, the following screens appears:

- Specify WebLogic Domain Detail
- Select Managed Instance
- Deinstallation Summary (Managed Instance)

M.2.2.1 Specify WebLogic Domain Detail

Specify the WebLogic Domain credentials:

- **Domain Host Name**

  The name of the system on which the WebLogic Domain is running.

- **Domain Port No**

  Listen port number of the domain. The default port number is `7001`.

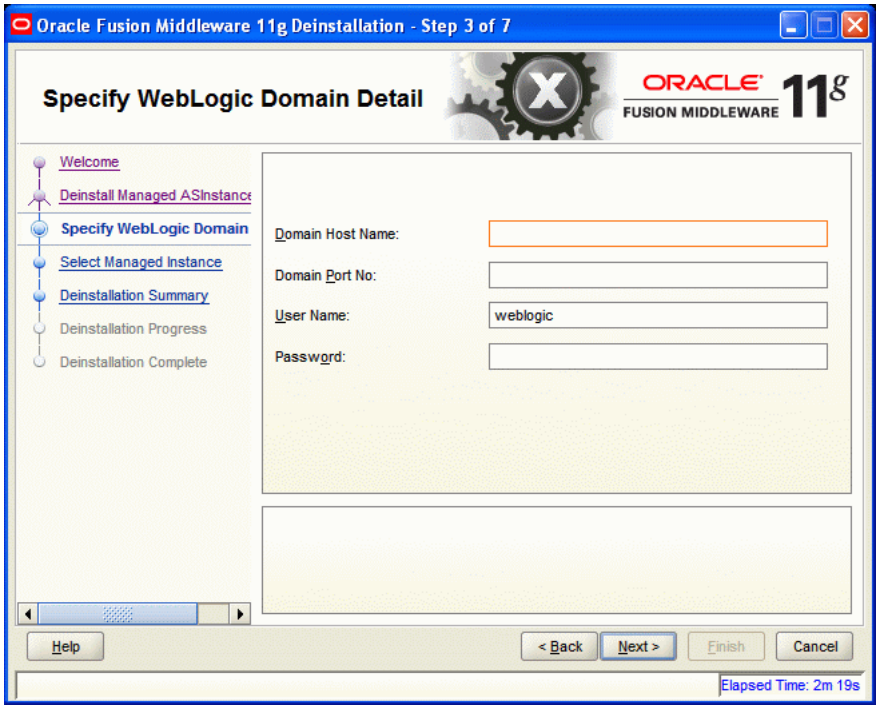
- **User Name**

  The WebLogic Domain user name.

- **Password**

  The password of the WebLogic Domain user.

Figure M–4 Specify WebLogic Domain Detail Screen

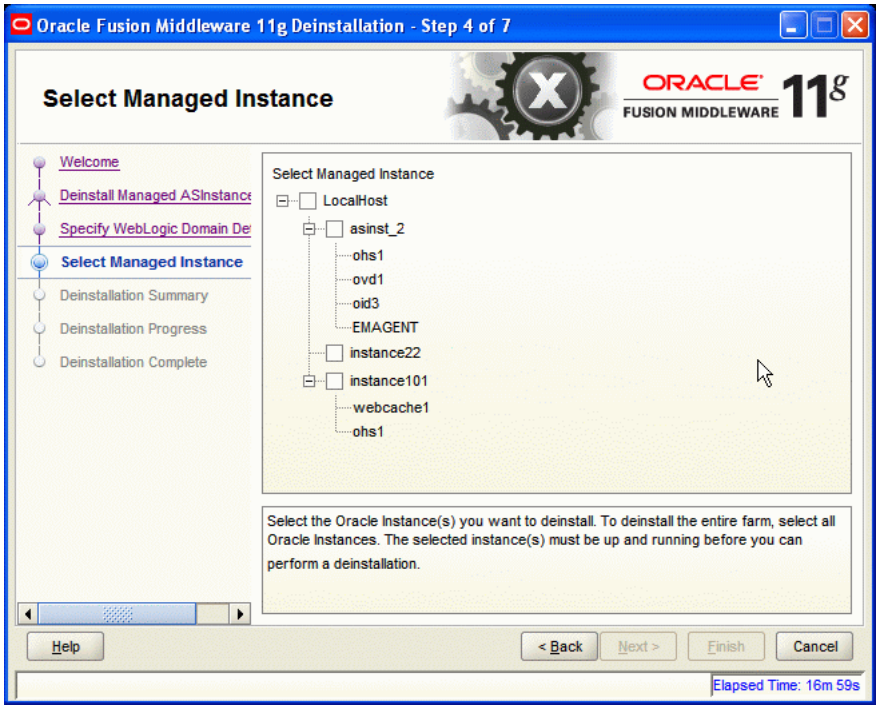


Click **Next** to continue.

M.2.2.2 Select Managed Instance

Select the managed instance you want to deinstall.

Figure M–5 Select Managed Instance Screen

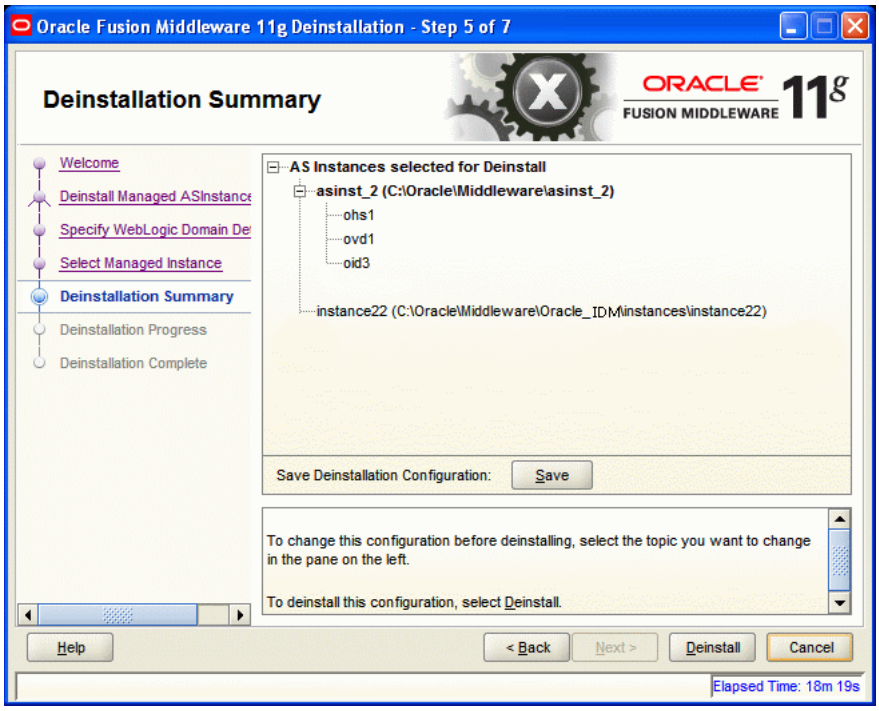


Click **Next** to continue.

M.2.2.3 Deinstallation Summary (Managed Instance)

Verify that the specified instance is the one you want to deinstall.

Figure M–6 Deinstallation Summary Screen



Click **Deinstall** to start the deinstallation process.

M.2.3 Option 3: Deinstall Unmanaged ASInstances

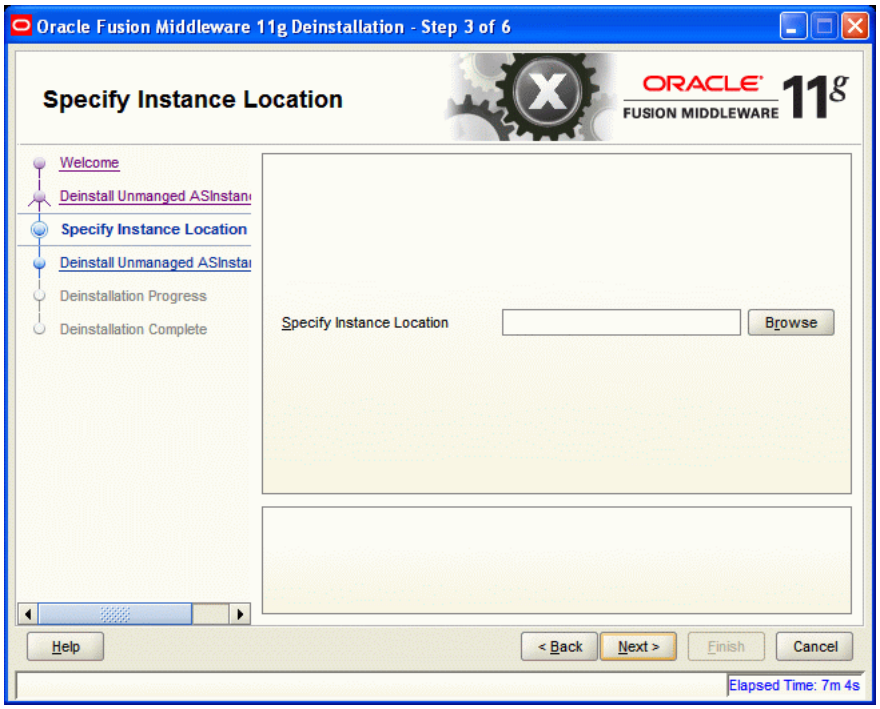
If you selected **Deinstall Unmanaged ASInstances** on the Select Deinstallation Type screen, the following screen appears:

- Specify Instance Location
- Deinstallation Summary (Unmanaged ASInstance)

M.2.3.1 Specify Instance Location

Specify the full path to your Oracle Instance directory. If you are unsure, click **Browse** to find this directory on your system.

Figure M–7 Specify Instance Location Screen

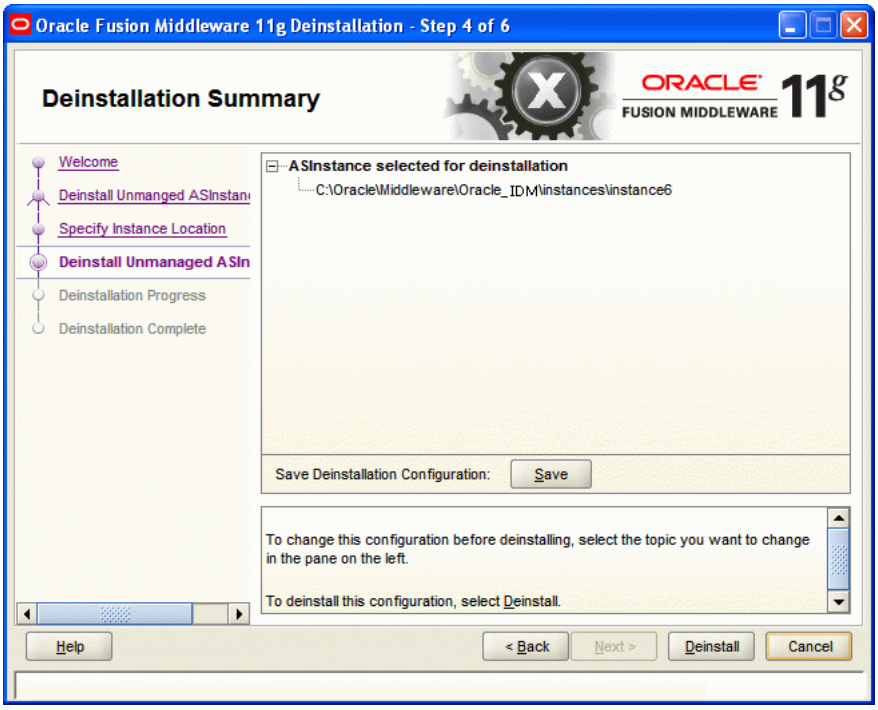


Click **Next** to continue.

M.2.3.2 Deinstallation Summary (Unmanaged ASInstance)

Verify that the specified instance is the one you want to deinstall.

Figure M–8 Deinstallation Summary Screen

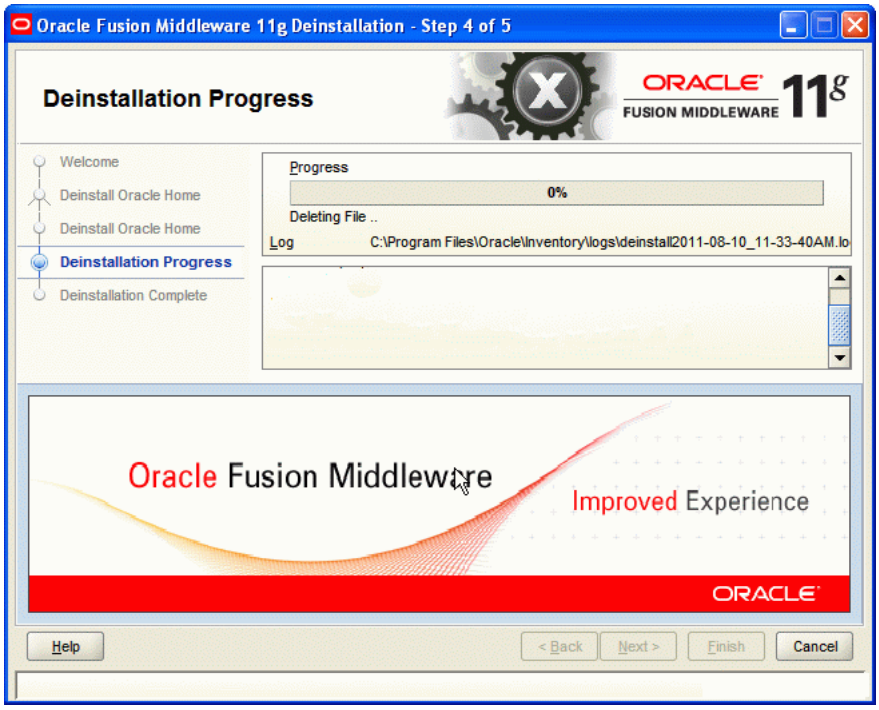


Click **Deinstall** to start the deinstallation process.

M.3 Deinstallation Progress

This screen shows you the progress of the deinstallation.

Figure M–9 Deinstallation Progress Screen



If you want to quit before the deinstallation is completed, click **Cancel**.

M.4 Deinstallation Complete

This screen summarizes the deinstallation that was just completed.

Figure M–10 Deinstallation Complete Screen

Click **Finish** to dismiss the deinstaller.