Oracle® Fusion Middleware

Installation Guide for Oracle Identity and Access Management

11*g* Release 2 (11.1.2.3.0)

E56489-03

January 2016

This guide explains how to install and configure Oracle Identity and Access Management 11*g* Release 2 (11.1.2.3.0) components.

ORACLE

Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management, 11*g* Release 2 (11.1.2.3.0)

E56489-03

Primary Author: Phil Stubbs

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, John Boyer, 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, Viral Kamdar, Tim Melander, Simon Kissane, Nisha Singh

Contents

Part II Installing and Configuring Oracle Identity and Access Management (11.1.2.3.0)

3 Installing and Configuring Oracle Identity and Access Management (11.1.2.3.0)

4 Configuring Oracle Identity Manager

5 Configuring Oracle Access Management

8 Configuring Oracle Privileged Account Manager

9 Configuring Oracle Access Management Mobile and Social

10 Configuring Oracle Mobile Security Suite

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

12 Verifying Your Environment Using the Environment Health Check Utility

Preface

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

Audience

The *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 the *Installation Guide for Oracle Identity Management*.

Documentation Accessibility

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

Access to Oracle Support

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

Related Documents

This section identifies additional documents related to Oracle Identity 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

- *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 Administering Oracle Identity Manager

Oracle Access Management

Oracle Fusion Middleware Administrator's Guide for Oracle Access Management

Oracle Adaptive Access Manager

Oracle Fusion Middleware Administering Oracle Adaptive Access Manager

Oracle Privileged Account Manager

Oracle Fusion Middleware Administering 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 Administering Oracle Entitlements Server

Oracle Mobile Security Suite

Oracle Fusion Middleware Administering Oracle Mobile Security Suite

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 (11.1.2.3.0) 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 (11.1.2.3.0).

This chapter includes the following topics:

1.1 Overview of Oracle Identity and Access Management 11*g* Release 2 (11.1.2.3.0)

Oracle Identity and Access Management 11*g* Release 2 (11.1.2.3.0) includes the following components:

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

> **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 *Installing Oracle Unified Directory*.

1.2 Additional 11*g* Release 2 (11.1.2.3.0) Deployment Information

This topic describes additional sources for 11*g* Release 2 (11.1.2.3.0) deployment information, including documentation on the following subjects:

- Upgrading to Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0)
- Migrating to Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0)
- Installing Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0) for High Availability

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

1.2.1 Upgrading to Oracle Identity and Access Management 11*g* Release 2 (11.1.2.3.0)

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 (11.1.2.3.0). To upgrade an Oracle Identity and Access Management component that is earlier than 11*g*, refer to the *Upgrade Guide for Oracle Identity and Access Management*.

1.2.2 Migrating to Oracle Identity and Access Management 11*g* Release 2 (11.1.2.3.0)

This guide does not explain how to migrate to Oracle Identity and Access Management 11*g* Release 2 (11.1.2.3.0) 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 (11.1.2.3.0) for High Availability

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

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

1.3 Silent Installation

In addition to the standard graphical installation option, you can perform a 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 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 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 (11.1.2.3.0) components.
2. Verify the installation was successful.
3. Get started with the component after installation.

This guide covers the most common, certified Oracle Identity 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 Privileged Account Manager, Oracle Access Management Mobile and Social, and Oracle Mobile Security Suite by using the Oracle Identity and Access Management 11*g* Release 2 (11.1.2.3.0) 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 (11.1.2.3.0):

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 (11.1.2.3.0)," for general installation and configuration information which applies to all Oracle Identity and Access Management 11*g* Release 2 (11.1.2.3.0) 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 (11.1.2.3.0).

This chapter discusses the following topics:

2.1 Reviewing System Requirements and Certification

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

- *Oracle Fusion Middleware System Requirements and Specifications for Oracle Identity and Access Management*

  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 might 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. You create the Oracle Middleware Home when you install Oracle WebLogic Server. The Oracle Middleware Home directory is commonly referred to as *MW_HOME*.

Note that it is recommended to create and use a separate Middleware home for each Oracle Identity and Access Management component you are installing.

For example,

ORACLE_BASE`/products/fmw_oim`

Note: *ORACLE_BASE* is the base directory under which Oracle products are installed. For example, `/u01/oracle`.

2.3.2 Oracle Home Directory

Identify 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 default name for the Oracle home directory is `Oracle_IDM1`.

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`)*. However, it is recommended that you create your domain home and application home outside of both the Middleware home and Oracle home directories, so that in the event you need to patch either the Middleware home or Oracle home, your domain and application information would remain untouched.

The Domain home directory is referenced as *`DOMAIN_HOME`* in this guide and includes all folders up to and including the domain name. For example, on a Linux or UNIX operating system, if you specified `/u01/oracle/admin/oam/user_projects/domains` as your Oracle Access Management domain location and `oam_domain` as your domain name, *`DOMAIN_HOME`* would be used in the documentation to refer to `/u01/oracle/admin/oam/user_projects/domains/oam_domain`.

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. For example, *ORACLE_BASE*/products/fmw_oam/wlserver_10.3. In examples, it is identified with the *WL_HOME* variable.

Note: *ORACLE_BASE* is the base directory under which Oracle products are installed. For example, /u01/oracle.

2.4 Determining Port Numbers

If you want to install an Oracle Identity and Access Management 11*g* Release 2 (11.1.2.3.0) 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 Linux or UNIX systems and to the *ORACLE_INVENTORY_LOCATION*\logs directory on Windows systems.

On Linux or 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

2.6 Verifying Your Database Password Policies

Before you install the required database schemas, review your current database password policies. In particular, review the password expiration policies. It is important that passwords for the required schemas do not expire. For more information, see Appendix G.3, "Password for OAM Schema on Oracle Database 11g Expires Every 180 Days."

Part II

Installing and Configuring Oracle Identity and Access Management (11.1.2.3.0)

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 Privileged Account Manager
- Oracle Access Management Mobile and Social
- Oracle Mobile Security Suite

Part II contains the following chapters:

3

Installing and Configuring Oracle Identity and Access Management (11.1.2.3.0)

This chapter explains how to install and configure Oracle Identity and Access Management.

It includes the following topics:

- Installation and Configuration Roadmap
- Installing and Configuring Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0)

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 (11.1.2.3.0) 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. Then, obtain the Oracle Fusion Middleware Software.	For more information, see *Oracle Fusion Middleware Download, Installation, and Configuration ReadMe*. Also, see Section 3.2.1, "Obtaining the Oracle Fusion Middleware Software."
3	Install a certified JDK.	For more information, see Section 3.2.2, "Installing a Certified JDK."
4	Review the Database requirements.	For more information, see Section 3.2.3, "Database Requirements." Note that for Oracle Identity Manager configurations that use Oracle Databases, some of the Oracle Database versions require patches. For more information, see Section 3.2.3.1, "Oracle Database Patch Requirements for Oracle Identity Manager." Also, see Section 3.2.4, "Optional: Enabling TDE in Database for Oracle Access Management."

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

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 3.2.5, "Creating Database Schemas Using the Oracle Fusion Middleware Repository Creation Utility (RCU)". **Notes:** If you are configuring Oracle Access Management Mobile and Social standalone, skip this step. If you are configuring Oracle Privileged Account Manager, Oracle Privileged Account Manager schema must be created by a Database user with `SYSDBA` privileges. If you are configuring 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). ▪ 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 D, "Creating Oracle Entitlement Server Schemas for Apache Derby".
6	Install Oracle WebLogic Server and create a Middleware Home.	For more information, see Section 3.2.6, "Installing Oracle WebLogic Server and Creating a Middleware Home". Also, Oracle WebLogic Server 11*g* Release 1 (10.3.6) requires some patches that must be applied on the WebLogic Server Middleware home. For more information, see Section 3.2.6.1, "Applying Mandatory Patches for Oracle WebLogic Server."
7	For Oracle Identity Manager users only: Install Oracle SOA Suite 11*g* Release 1 (11.1.1.9.0).	For more information, see Section 3.2.7, "Installing Oracle SOA Suite (Oracle Identity Manager Users Only)".
8	Install the Oracle Identity and Access Management 11*g* software.	For more information, see Section 3.2.8, "Installing Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0)".
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 3.2.9, "Configuring Oracle Identity and Access Management (11.1.2.3.0) Products".
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."

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

No.	Task	Description
11	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.	For more information, see Section 3.2.11, "Configuring Oracle Identity Manager Server and Design Console".
12	Start the servers.	You must start the Administration Server and all Managed Servers. For more information, see Section C.1, "Starting the Stack".
13	Run the Oracle Identity and Access Environment Health Check Utility to verify your installation and configuration.	For more information, see Section 3.2.13, "Verifying Your Environment Using the Environment Health Check Utility."

3.2 Installing and Configuring Oracle Identity and Access Management 11*g* Release 2 (11.1.2.3.0)

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
- Installing a Certified JDK
- Database Requirements
- Optional: Enabling TDE in Database for Oracle Access Management
- Creating Database Schemas Using the Oracle Fusion Middleware Repository Creation Utility (RCU)
- Installing Oracle WebLogic Server and Creating a Middleware Home
- Installing Oracle SOA Suite (Oracle Identity Manager Users Only)
- Installing Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0)
- Configuring Oracle Identity and Access Management (11.1.2.3.0) Products
- Configuring Database Security Store for an Oracle Identity and Access Management Domain
- Configuring Oracle Identity Manager Server and Design Console
- Starting the Servers
- Verifying Your Environment Using the Environment Health Check Utility

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 11*g* Release 1 (11.1.1.9.0)
- Oracle Identity and Access Management Suite
- Oracle SOA Suite 11*g* Release 1 (11.1.1.9.0) (required for Oracle Identity Manager only)
- Oracle Entitlements Server Client (required for Oracle Entitlements Server only)
- Oracle Mobile Security Access Server (required for Oracle Mobile Security Suite only)

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

3.2.2 Installing a Certified JDK

Before you can install Oracle Identity and Access Management, you must download and install a supported Java Development Kit (JDK) on your system.

You should always verify the required JDK version by reviewing the certification information on the *Oracle Fusion Middleware Supported System Configurations* page.

The JDK can be downloaded from the Java SE Development Kit 7 Downloads page on Oracle Technology Network (OTN).

Note: For more information about JDK version requirements, see the "Oracle WebLogic Server and JDK Considerations " topic in the *Oracle Fusion Middleware System Requirements and Specifications for Oracle Identity and Access Management* 11*g* Release 2 (11.1.2) document.

3.2.3 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 components. The database does not have to be on the same system where you are installing the Oracle Identity and Access Management components.

Notes:

- 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.

3.2.3.1 Oracle Database Patch Requirements for Oracle Identity Manager

Some of the Oracle Database versions require patches. To identity 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 *Release Notes for Oracle Identity Management*.

3.2.4 Optional: Enabling TDE in Database for Oracle Access Management

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 3.2.5, "Creating Database Schemas 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*.

3.2.5 Creating Database Schemas 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 Mobile Security Suite
- 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 (11.1.2.3.0) components, use the 11*g* Release 1 (11.1.1.9.0) 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*.

  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 Oracle 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 following information about your database ready:

- Database Type
- Database Host Name
- Database Port
- Database Service Name
- Database User Name
- Database User's Password
- Database User's Role

To run RCU and create the required schemas in the database, perform the following steps:

1. After obtaining the proper version of RCU and downloading the `.zip` file, extract the contents to a directory of your choice. This directory will be referred to as the *`RCU_HOME`* directory.
2. Start RCU from the `bin` directory inside the `RCU_HOME` directory.

   On Linux:

   ```
   cd RCU_HOME/bin
   ./rcu
   ```

   On Windows:

```
cd RCU_HOME\bin
rcu.bat
```

3. On the Welcome screen, click **Next.**
4. On the Create Repository screen, select **Create** to load the component schemas into an existing database, and then click **Next.**
5. On the Database Connection Details screen, specify the connection details for your database, and then click **Next**.

> **Note:** For more information about the options on this screen, see "Database Connection Details" in the *Oracle Fusion Middleware Repository Creation Utility User's Guide*.

6. A separate dialog window will appear while RCU checks database connectivity and some database prerequisites. When the database checking has passed without errors, click **OK** to dismiss the dialog window and go to the next screen.
7. On the Select Components screen, specify a prefix that you want to use for your schemas and select the components for which you want to create schemas in the database.

> **Notes:**
>
> - For more information about the options on this screen, see "Select Components (for Create Operation)" in the *Oracle Fusion Middleware Repository Creation Utility User's Guide*
> - For more information about custom prefixes, see "Using Custom Prefixes" in the *Oracle Fusion Middleware Repository Creation Utility User's Guide*.
> - For Oracle Identity Manager, Oracle Access Manager, and Oracle Adaptive Access Manager schemas on the same database, it is recommended to provide different schema prefixes for these schemas to make sure that the **AS Common Schemas - Oracle Platform Security Services** and **AS Common Schemas - Metadata Services** schemas are not shared.

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 schemas 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 and BPM Infrastructure - SOA Infrastructure**
  - **SOA and BPM Infrastructure - User Messaging Service**
  - **AS Common Schemas - Oracle Platform Security Services**
  - **AS Common Schemas - Metadata Services**
  - **Oracle Business Intelligence - Business Intelligence Platform**

- 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 H, "Oracle Adaptive Access Manager Partition Schema Reference".

- For Oracle Access Management only, select the **Identity Management - Oracle Mobile Security Manager** schema.

  By default, Oracle Mobile Security Suite is installed (but not fully configured) with Oracle Access Management. You can choose to configure Oracle Access Management only or configure Oracle Access Management with Oracle Mobile Security Suite. For both configuration options, you must select the **Identity Management - Oracle Mobile Security Manager** schema.

  When you select the **Identity Management - Oracle Mobile Security 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**
  - **Identity Management - Oracle Access Manager**

Notes:

- 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 3.2.4, "Optional: Enabling TDE in Database for Oracle Access Management."
- If you manually select the **Identity Management - Oracle Access Manager** schema only, the **Identity Management - Oracle Mobile Security Manager** schema will not be selected by default. In this case, you must also manually select the **Identity Management - Oracle Mobile Security Manager** schema because when you install and configure Oracle Access Management in a WebLogic domain, the Oracle Mobile Security Manager server is installed and configured in the domain by default.

- 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.

Click **Next**.

8. A separate dialog window will appear while RCU checks component prerequisites. When the component prerequisite checking has passed without errors, click **OK** to dismiss the dialog window and go to the next screen.
9. On the Schema Passwords screen, specify how you want to set the schema passwords on your database. Then, enter and confirm your passwords for the main and additional (auxiliary) schema users. Click **Next**.

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.

10. On the Map Tablespaces screen, configure the desired tablespace mapping for the schemas you want to create, and then click **Next**.

    A separate dialog window will appear asking you to confirm that you want to create these tablespaces. Click **OK** to proceed and dismiss the dialog window.

A second dialog window will appear showing the progress of the tablespace creation. After this is complete, click **OK** to dismiss this window and go to the next screen.

11. Review the information on the Summary screen, and click **Create** to begin schema creation.

    A separate dialog window will appear showing the progress of the schema creation. After this is complete, the Completion Summary screen will appear.

12. On the Completion Summary screen, note the location of the log files, and then click **Close** to dismiss RCU.

3.2.6 Installing Oracle WebLogic Server and Creating a Middleware Home

Before you install Oracle Identity and Access Management 11*g* Release 2 (11.1.2.3.0) components, you must ensure that you have installed Oracle WebLogic Server and created a Middleware Home directory.

Notes:

- 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 you are using a JDK version that is supported and certified with Oracle Identity and Access Management 11*g* Release 2 (11.1.2.3.0). For more information, see Section 3.2.2, "Installing a Certified JDK."
- Before you install Oracle WebLogic Server, ensure that your system environment meets the requirements for the installation. For installation requirements, see "Installation Prerequisites" in the *Oracle WebLogic Server Installation Guide*.

To install Oracle WebLogic Server, perform the following steps:

1. Start the Oracle WebLogic Server Installer, as described in "Starting the Installation Program in Graphical Mode" in the *Oracle WebLogic Server Installation Guide*.
2. On the Welcome screen, click **Next**.
3. On the Choose Middleware Home Directory screen, select **Create a New Middleware Home**.

   Enter a location for the Middleware home directory. Note that it is recommended to create and use a separate Middleware home for each Oracle Identity and Access Management component you are installing.

   For example,

   ORACLE_BASE`/products/fmw_oim`

   Note: *ORACLE_BASE* is the base directory under which Oracle products are installed. For example, `/u01/oracle`.

   Click **Next**.

4. Specify whether you want to register the product installation with My Oracle Support. By registering, Oracle Support notifies you immediately of any security updates that are specific to your installation. Click **Next.**

   If you chose not to register, a separate dialog window appears notifying you that you have not provided an email address. Click **Yes** to continue. An **Are you sure?** dialog window appears. Click **Yes** to continue. A **Connection failed** window appears. Select the **I wish to remain uninformed of security issues in my configuration or this machine has no Internet access** check box and click **Continue**.

5. On the Choose Install Type screen, select **Typical**.

   Click **Next**.

6. On the JDK Selection screen, select the JDK.

   Click **Next.**

7. On the Choose Product Installation Directories screen, accept the default product installation directories.

   Click **Next**.

8. On the Installation Summary screen, click **Next.**

   Monitor the progress of your installation.

9. On the Installation Complete screen, deselect **Run Quickstart**.

   Click **Done**.

For complete information about installing Oracle WebLogic Server, see the *Oracle WebLogic Server Installation Guide*.

After installing Oracle WebLogic Server, you must apply mandatory WebLogic Server patches on the Middleware home. For more information, see Section 3.2.6.1, "Applying Mandatory Patches 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.

3.2.6.1 Applying Mandatory Patches for Oracle WebLogic Server

After you have installed Oracle WebLogic Server 11*g* Release 1 (10.3.6) and created a Middleware home directory, there are some mandatory patches that you must apply to your WebLogic Server Middleware home to fix specific issues with Oracle WebLogic Server 11*g* Release 1 (10.3.6).

To identify the required patches that you must apply for Oracle WebLogic Server, see "Downloading and Applying Required Patches" in the *Oracle Fusion Middleware Infrastructure Release Notes*.

The WebLogic Server patches listed in the release notes are available from My Oracle Support. The patching instructions are mentioned in the `README.txt` file that is provided with each patch.

3.2.7 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 (11.1.1.9.0). Note that only Oracle Identity Manager requires Oracle SOA Suite. This step is required because Oracle Identity Manager uses process work flows in Oracle SOA Suite to manage request approvals.

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

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

3.2.8 Installing Oracle Identity and Access Management 11*g* Release 2 (11.1.2.3.0)

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 Entitlements Server, Oracle Privileged Account Manager, Oracle Access Management Mobile and Social, and Oracle Mobile Security Suite.

It includes the following sections:

- Products Installed
- Dependencies
- Procedure

3.2.8.1 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 (11.1.2.3.0) 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 *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 *Administrator's Guide for Oracle Access Management*.

- Oracle Adaptive Access Manager

  Note: For Oracle Identity and Access Management 11.1.2.3.0, Oracle Adaptive Access Manager includes two components

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

- 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 7.5, "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 *Administering Oracle Privileged Account Manager*.

- Oracle Mobile Security Suite

  Note: When you are installing Oracle Identity and Access Management, only the Oracle Mobile Security Manager component of Oracle Mobile Security Suite is installed.

  To install and configure Oracle Mobile Security Access Server, see Section 10.12, "Installing Oracle Mobile Security Access Server."

3.2.8.2 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*g* Release 1 (11.1.1.9.0) (required for Oracle Identity Manager only)
- JDK

3.2.8.3 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 Entitlements Server, Oracle Privileged Account Manager, Oracle Access Management Mobile and Social, and Oracle Mobile Security Suite:

1. Start the Oracle Identity and Access Management Installer by executing one of the following commands:

On Linux or 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_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.

After you start the Installer, the Welcome screen appears.

2. Click **Next** on the Welcome screen. The Install Software Updates screen appears.
3. On the Install Software Updates screen, select whether or not you want to search for updates. Click **Next.** The Prerequisite Checks screen appears.
4. If all prerequisite checks pass inspection, click **Next**. The Specify Installation Location screen appears.
5. 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. For example, `/u01/oracle/products/fmw_oam`.

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.

---

6. 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. The default name of the Oracle home directory for Oracle Identity and Access Management is `Oracle_IDM1`.

   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.

7. 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 pane 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**.

8. 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 **Next**.

> **Note:** If you cancel or abort when the installation is in progress, you must manually delete the *IAM_HOME* directory before you can reinstall the Oracle Identity and Access Management software.
>
> To invoke online help at any stage of the installation process, click the **Help** button on the installation wizard screens.

9. 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.

10. Check the directory structure after installing Oracle Identity and Access Management to verify your installation.

    This installation process copies the Oracle Identity and Access Management software to your system and creates an Oracle Home directory for Oracle Identity and Access Management, such as `Oracle_IDM1`, 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".

    After installing the Oracle Identity and Access Management software, you must proceed to Section 3.2.9, "Configuring Oracle Identity and Access Management (11.1.2.3.0) Products," to configure Oracle Identity and Access Management products in a new or existing WebLogic domain.

3.2.9 Configuring Oracle Identity and Access Management (11.1.2.3.0) 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 11.1.2.3.0 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 (11.1.2.3.0) 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 Linux or 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 *Understanding Domain Configuration for Oracle WebLogic Server* guide for more information about Oracle WebLogic Server administration domains.
>
> In addition, see the *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 Manager"
- Chapter 5, "Configuring Oracle Access Management"
- Chapter 6, "Configuring Oracle Adaptive Access Manager"
- Chapter 7, "Configuring Oracle Entitlements Server,"
- Chapter 8, "Configuring Oracle Privileged Account Manager"
- Chapter 9, "Configuring Oracle Access Management Mobile and Social"
- Chapter 10, "Configuring Oracle Mobile Security Suite"

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

After configuring the WebLogic Server Administration Domain for Oracle Identity and Access Management components and before starting the Oracle WebLogic Administration Server, you must configure the Database Security Store by running the configureSecurityStore.py script. For more information, see Chapter 11, "Configuring Database Security Store for an Oracle Identity and Access Management Domain."

3.2.11 Configuring Oracle Identity Manager Server and Design Console

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 4.7, "Configuring Oracle Identity Manager Server".

You can also configure Oracle Identity Manager Design Console, if required. For more information, see Section 4.8, "Optional: Configuring Oracle Identity Manager Design Console."

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.

3.2.13 Verifying Your Environment Using the Environment Health Check Utility

After installing and configuring Oracle Identity and Access Management, you can run the Oracle Identity and Access Environment Health Check Utility to perform various validation checks against your environment and verify your installation and configuration. For more information about the Environment Health Check Utility and how to run the utility, see Chapter 12, "Verifying Your Environment Using the Environment Health Check Utility."

4

Configuring Oracle Identity Manager

This chapter explains how to configure Oracle Identity Manager.

It includes the following topics:

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

4.1 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 Privileged Account Manager, Oracle Access Management Mobile and Social, and Oracle Mobile Security Suite. You can specify any path 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 *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 and Oracle Identity Manager Design Console (on Windows only).

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

  Note that Oracle Identity Manager requires Oracle SOA Suite 11*g* Release 1 (11.1.1.9.0), 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 and Oracle Access Management are configured in different WebLogic Server domains (split domain).

4.2 Configuration Roadmap for Oracle Identity Manager

Table 4–1 lists the tasks for configuring Oracle Identity Manager.

Table 4–1 Configuration Flow for Oracle Identity Manager

No.	Task	Description
1	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, "Creating a new WebLogic Domain for Oracle Identity Manager, SOA, and BI Publisher"
2	Configure the Database Security Store.	For more information, see Section 4.4, "Configuring the Database Security Store".
3	Start the servers.	You must start the Administration Server and the SOA Managed Server. For more information, see Section 4.5, "Starting the Servers".
4	Review the Oracle Identity Manager Server and Design Console configuration scenarios.	For more information, see Section 4.6, "Overview of Oracle Identity Manager Configuration".

Table 4–1 (Cont.) Configuration Flow for Oracle Identity Manager

No.	Task	Description
5	Configure Oracle Identity Manager Server.	For more information, see Section 4.7, "Configuring Oracle Identity Manager Server".
6	Optional: Install and Configure only Oracle Identity Manager Design Console on Windows.	For more information, see Section 4.8, "Optional: Configuring Oracle Identity Manager Design Console".
7	Complete the post-installation tasks.	Complete the following post-installation tasks: ■ Section 4.9, "Verifying the Oracle Identity Manager Installation" ■ Section 4.10, "Changing Memory Settings for Oracle Identity Manager" ■ Section 4.11, "Setting Up Integration with Oracle Access Management" ■ Section 4.12, "List of Supported Languages" ■ Section 4.13, "Getting Started with Oracle Identity Manager After Installation"

4.3 Creating a new WebLogic Domain for Oracle Identity Manager, SOA, and BI Publisher

This topic describes how to create a new WebLogic domain for Oracle Identity Manager, SOA, and BI Publisher. 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 install Oracle Identity Manager in an environment where you might 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.

4.3.2 Components Deployed

Performing the configuration in this section installs the following components:

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

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* Release 2 (11.1.2.3.0) software
- Installation of Oracle SOA Suite 11*g* Release 1 (11.1.1.9.0)
- Database schemas for Oracle Identity Manager, Oracle SOA 11*g* Suite, and Oracle BI Publisher.

4.3.4 Procedure

Complete the following steps to create a new WebLogic domain for Oracle Identity Manager, SOA, and BI Publisher.

1. Review the section Important Notes Before You Start Configuring Oracle Identity Manager.
2. Run the *IAM_HOME*`/common/bin/config.sh` script (on Linux or 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 Mobile Security Suite.

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]**
   - **Oracle BI Publisher - 11.1.1.6.0 [oracle_bip]**
   - **Oracle BI JDBC - 11.1.1.9.0 [oracle_bip]**
   - **Oracle OPSS Metadata for JRF - 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.

   For example,

   - **Domain name:** `oim_domain`
   - **Domain location:** *`ORACLE_BASE`*`/admin/oim/user_projects/domains`
   - **Application location:** *`ORACLE_BASE`*`/admin/oim/user_projects/applications`

   Notes:

   - *`ORACLE_BASE`* is the base directory under which Oracle products are installed. For example, `/u01/oracle`.
   - The default locations for the domain home and application home are *`MW_HOME`*`/user_projects/domains` and *`MW_HOME`*`/user_projects/applications`, respectively. However, it is recommended that you create your domain and application home directories outside of both the Middleware home and Oracle home.

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 mode under **WebLogic Domain Startup Mode**. Click **Next**.
8. The Configure JDBC Component Schema screen appears. This screen displays a list of the following component schemas:
   - OIM Schema
   - SOA Infrastructure
   - User Messaging Service
   - BIP Schema
   - OIM MDS Schema
   - OWSM MDS Schema
   - SOA MDS Schema
   - 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.

   If the test fails, click **Previous**, correct the issue, and try again.

   After the test succeeds, click **Next**. 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**. Select the relevant check boxes and click **Next**.
11. Use the Configure the Administration Server screen to 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.
13. Configure Managed Servers.

    When you first enter the Configure Managed Servers screen, three default Managed Servers (`soa_server1`, `oim_server1`, and `bi_server1`) have been created for you and have been automatically assigned to default ports. Change the default Managed Server names to the following:

- For the SOA Server entry (`soa_server1`), change the name to `WLS_SOA1`.
- For the Oracle Identity Manager Server entry (`oim_server1`), change the name to `WLS_OIM1`.
- For the BI Publisher Server entry (`bi_server1`), change the name to `WLS_BIP1`

Notes:

- On the Configure Managed Servers screen, if the **Listen address** for the SOA Managed Server and the BI Publisher Managed Server are not specified, then it is assumed that the SOA server and the BI Publisher server are running on a local host.

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

- For more information, see "Configure Managed Servers" in *Creating Domains Using the Configuration Wizard*.

These server names will be referenced throughout this document. If you choose different names, then be sure to replace them as needed.

Click **Next**.

14. On the Configure Clusters screen, click **Add** to create three clusters with the following names for SOA, Oracle Identity Manager, and BI Publisher:
    - `soa_cluster`
    - `oim_cluster`
    - `bi_cluster`

    Leave all other fields at the default settings and click **Next.**

    Note: 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 *High Availability Guide*.

    ---

15. On the Assign Servers to Clusters screen, assign the Managed Servers to clusters as follows:
    - Assign the SOA Managed Server (**WLS_SOA1**) to **soa_cluster**.
    - Assign the Oracle Identity Manager Managed Server (**WLS_OIM1**) to **oim_cluster**.
    - Assign the BI Publisher Managed Server (**WLS_BIP1**) to **bi_cluster.**

    Click **Next**.

16. Use the Configure Machines screen to create and configure machines in the domain, 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.

Note: For more information about the options on this screen, see "Configure Machines" in *Creating Domains Using the Configuration Wizard*.

Click **Next.**

17. On the Assign Servers to Machines screen, assign the Administration Server to a machine.
18. Assign the newly created Managed Servers, such as `WLS_OIM1`, `WLS_SOA1`, and `WLS_BIP1`, to a machine.

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

    By default, a new WebLogic domain to support Oracle Identity Manager is created in the *`MW_HOME`*`\user_projects\domains` directory (on Windows). On Linux or UNIX, the domain is created in the *`MW_HOME`*`/user_projects/domains` directory, by default.

4.4 Configuring the Database Security Store

After configuring Oracle Identity Manager and SOA in a new WebLogic administration domain and before starting the Oracle WebLogic Administration Server, you must configure the Database Security Store by running the `configureSecurityStore.py` script. For more information, see Chapter 11, "Configuring Database Security Store for an Oracle Identity and Access Management Domain."

4.5 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 *Administering 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 and wait for the SOA server to come up. The SOA server is started when the following message appears: `SOA Platform is running and accepting requests`. Then, start the Oracle Identity Manager server.

4.6 Overview of Oracle Identity Manager Configuration

This section discusses the following topics:

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

4.6.1 Before Configuring Oracle Identity Manager Server or Design Console

Before configuring Oracle Identity Manager using the Oracle Identity Manager Configuration 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 Oracle Identity Manager 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

4.6.1.1 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 3.2.3, "Database Requirements".
2. Creating and loading the required schemas in the database. For more information, see Section 3.2.5, "Creating Database Schemas 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 3.2.6, "Installing Oracle WebLogic Server and Creating a Middleware Home".

4. Installing Oracle SOA Suite 11*g* Release 1 (11.1.1.9.0) under the same Middleware Home directory. For more information, see Section 3.2.7, "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 Access Management Mobile and Social, and Oracle Mobile Security Suite) under the Middleware Home directory. For more information, see Section 3.2.8, "Installing Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0)".
6. Creating a new WebLogic domain or extending an existing Oracle Identity and Access Management domain for Oracle Identity Manager, Oracle SOA Suite, and Oracle BI Publisher. For more information, see Section 4.3, "Creating a new WebLogic Domain for Oracle Identity Manager, SOA, and BI Publisher".
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".

4.6.1.2 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 (11.1.2.3.0) software containing 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 Mobile Security Suite. For information, see Section 3.2.8, "Installing Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0)".

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 4.7, "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.

4.6.2 Oracle Identity Manager Configuration Scenarios

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

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 or Design Console. 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 Design Console on a Single Windows Machine

4.6.2.1 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.

4.6.2.2 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 4.7, "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 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 4.8, "Optional: Configuring Oracle Identity Manager Design Console".

4.6.2.3 Scenario 2: Oracle Identity Manager Server and Design Console on a Single Windows Machine

In this scenario, suitable for test environments, you install and configure Oracle Identity Manager Server and Design Console 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 4.7, "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 4.8, "Optional: Configuring Oracle Identity Manager Design Console".

4.7 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
- Enabling LDAP Sync After Installing and Configuring Oracle Identity Manager Server at a Later Point

4.7.1 Appropriate Deployment Environment

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

4.7.2 Components Deployed

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

4.7.3 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 3.2.8, "Installing Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0)".

4.7.4 Procedure

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

1. Ensure that all the prerequisites, described in Section 4.6.1.1, "Prerequisites for Configuring Oracle Identity Manager Server", are satisfied. In addition, see Section 4.1, "Important Notes Before You Start Configuring Oracle Identity Manager".
2. On the machine where the Administration Server is running, start the Oracle Identity Manager 11*g* Configuration Wizard by executing one of the following commands:

   On Linux or UNIX:

   ```
   IAM_HOME/bin/config.sh
   ```

   On Windows:

   ```
   IAM_HOME\bin\config.bat
   ```

   > **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 or Design Console.

   After you start the Oracle Identity Manager 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 or 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 3.2.5, "Creating Database Schemas 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 3.2.5, "Creating Database Schemas 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, the Oracle SOA Suite application, and the Oracle BI Publisher application are deployed. If you are setting up integration between Oracle Identity Manager and Oracle Access Manager, then the Oracle Access Manager application is configured in a different WebLogic Server domain.

   In the **Password** field, enter the WebLogic administrator password of the domain in which the Oracle Identity Manager application, the Oracle SOA Suite application, and the Oracle BI Publisher 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 six 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 the Oracle Identity Manager Managed Server is not front-ended with Oracle HTTP Server, you can provide the Oracle Identity Manager Managed Server URL.
    - For single node deployments where Oracle Identity Manager Managed Server is front-ended 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 front-ends the Oracle Identity Manager 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 the Oracle Identity Manager Managed Server is not front-ended with Oracle HTTP Server, this field can be left blank.
    - For deployments where there is no Single-Sign On (SSO) configured but the Oracle Identity Manager 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 Single-Sign On (SSO) is configured, provide the SSO URL where the Oracle Identity Manager user interface is available.
    - If you are planning to integrate Oracle Identity Manager with Oracle Access Management, it is recommended that you enter a value in the **OIM External Front End URL** field.
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.

    Note: You are not prompted to enter a password for the keystore on the OIM Server screen if the `default-keystore.jks` keystore already exists. Instead, the keystore password is already available in and automatically read from the Credential Store Framework (CSF). Specifically, you are not prompted to enter a keystore password for the following scenarios:
    - You are adding Oracle Identity Manager to an existing domain.
    - You have started the Oracle Access Management server prior to running the Oracle Identity Manager Configuration Wizard. Starting the Oracle Access Management server generates `default-keystore.jks` with a random password if the keystore does not exist.
15. In the **Confirm Keystore Password** field, enter the new password again.

16. Optional: To enable LDAP Sync, you must select the **Enable OIM for Suite integration** check box on the OIM Server screen. Select this check box if you are planning to integrate Oracle Identity Manager with Oracle Access Manager.

    When you select this option, the Oracle Identity Manager Configuration Wizard configures LDAP sync to synchronize identity store information between the Oracle Identity Manager database store and the Oracle Access Manager LDAP directory service.

    Notes:

    - If you are not planning to integrate Oracle Identity Manager with Oracle Access Manager, then do not select the **Enable OIM for Suite integration** check box.
    - If you want to enable LDAP Sync, before enabling LDAP Sync you must complete prerequisite steps to configure your LDAP directory. For more information, see Section 4.7.5, "Completing the Prerequisites for Enabling LDAP Synchronization."
    - Once LDAP Sync is enabled on the OIM Server screen and prerequisites are completed, you must continue to configure the Oracle Identity Manager Server. After you have configured the Oracle Identity Manager Server and exited the Oracle Identity Manager Configuration Wizard, you must run the LDAP Post-Configuration Utility. For more information, see Section 4.7.6, "Running the LDAP Post-Configuration Utility."

    After making your selections, click **Next** on the OIM Server screen.

17. If chose to enable LDAP Sync by selecting the **Enable OIM for Suite integration** check box on the OIM Server screen, 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
      - ODSEE/IPLANET
      - OUD
      - ACTIVE_DIRECTORY
      - OVD

      Note: IPLANET is also referred to as Oracle Directory Server Enterprise Edition (ODSEE) in this guide.

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

      For example: `oid1` for OID, `oud1` for OUD, and `iplanet1` for IPLANET.

    - **Server URL** - enter the LDAP URL in the format `ldap://`*`ldap_host`*`:`*`ldap_port`*.

      For Microsoft Active Directory, the LDAP URL must be a SSL URL.

- **Server User** - enter the user name for the Directory Server administrator.

  For example: `cn=oimAdminUser,cn=systemids,dc=example,dc=com`

- **Server Password** - enter the password for the Directory Server administrator.
- **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=example,dc=com`.
    - **LDAP RoleContainer Description** - enter a description for the default role container.
    - **LDAP Usercontainer** - enter a name for the container that will be used as a default container of users in the LDAP directory. You can configure isolation rules in Oracle Identity Manager to create users in different containers in LDAP. For example, `cn=users,cn=oracleAccounts,dc=example,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=example,dc=com`.

    After enabling LDAP synchronization for integrating Oracle Identity Manager with Oracle Access Management and after running the LDAP Post-Configuration Utility, you can verify it by using the Oracle Identity Manager Administration Console. For more information, see Section 4.7.7, "Verifying the LDAP Synchronization." Click **Next**.

19. If you did not select the **Enable OIM for Suite integration** check box 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 pane 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 the 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.

4.7.5 Completing the Prerequisites for Enabling LDAP Synchronization

If you are integrating Oracle Identity Manager with Oracle Access Management and want to enable LDAP Sync, before enabling LDAP Synchronization you must complete prerequisite steps to configure your LDAP directory.

To complete the prerequisites for enabling LDAP Sync, refer to the following topics in the *Integration Guide for Oracle Identity Management Suite*:

- "Completing the Prerequisites for Enabling LDAP Synchronization"
- "Creating OVD Adapters"

4.7.6 Running the LDAP Post-Configuration Utility

If you enabled LDAP Sync during the Oracle Identity Manager Server configuration, 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 LDAP Sync Incremental Reconciliation jobs.

For information on how to run the LDAP Post-Configuration Utility, see "Running the LDAP Post-Configuration Utility" in the *Integration Guide for Oracle Identity Management Suite*.

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 only required if you chose to enable LDAP Sync during the Oracle Identity Manager Server configuration.

4.7.7 Verifying the LDAP Synchronization

If you enabled and configured LDAP Sync during the Oracle Identity Manager Server configuration, verify the configuration of LDAP with Oracle Identity Manager. To verify the LDAP Synchronization, refer to "Verifying the LDAP Synchronization" in the *Integration Guide for Oracle Identity Management Suite*.

4.7.8 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 *Integration Guide for Oracle Identity Management Suite*.

4.8 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

4.8.1 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.

4.8.2 Components Deployed

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

4.8.3 Dependencies

The installation and configuration in this section depends on the installation of Oracle Identity and Access Management 11*g* software and on the configuration of Oracle Identity Manager Server. For more information, see Installing Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0) and Configuring Oracle Identity Manager Server.

4.8.4 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 by executing the following command:

   ```
   IAM_HOME\bin\config.bat
   ```

   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 or Design Console.

   After you start the Oracle Identity Manager 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 Manager Managed 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 pane 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.

4.8.5 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.

4.8.6 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.

4.8.7 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, `WLS_OIM1`). The Settings for `WLS_OIM1` 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/loginWorkflowRend
      erer.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.namin
      g.provider.url>
      ```

   c. Save the file and exit.

4.9 Verifying the Oracle Identity Manager Installation

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

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

You can verify your Oracle Identity Manager installation by:

- Checking the Oracle Identity Manager System Administration URL, such as http://*oim_host:oim_port*/sysadmin
- Checking the Oracle Identity Manager Self Service URL, such as http://*oim_host*:*oim_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://oim_host:oim_port/identity`

c. Navigate to **My Information** on the **Home** page of the **Self Service** tab. Modify any attribute and click **Apply**. This should raise a request. Logout from the Oracle Identity Manager Self Service console.

d. Log in to the Oracle Identity Manager Self Service Console as `xelsysadm`:

`http://oim_host:oim_port/identity`

e. Navigate to **Pending Approvals** on the **Home** page of the **Self Service** tab. In the list of tasks, verify whether the request has come for approval.

f. Click the task, and then click **Approve**.

g. Click the refresh icon.

h. Navigate to **Track Requests** on the **Home** page of the **Self Service** tab.

i. Click **Refresh**, and verify whether the request is completed.

j. Click the **Manage** tab in the top right corner, and navigate to **Users** on the **Home** page. 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.

4.10 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 Linux or 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 Oracle Identity Manager Server. For more information, see Appendix C.3, "Restarting Servers".

4.11 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 *Integration Guide for Oracle Identity Management Suite*.

4.12 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

4.13 Getting Started with Oracle Identity Manager After Installation

After installing Oracle Identity Manager, refer to "Oracle Identity System Administration Interface" in *Administering Oracle Identity Manager*.

5

Configuring Oracle Access Management

This chapter explains how to configure Oracle Access Management.

It includes the following topics:

5.1 Overview

Oracle Identity and Access Management 11*g* Release 2 (11.1.2.3.0) 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 *Administrator's Guide for Oracle Access Management*.

5.2 Important Note Before You Begin

Before you start configuring Oracle Access Management, 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 Privileged Account Manager, Oracle Access Management Mobile and Social, and Oracle Mobile Security Suite. You can specify any path for this Oracle home directory.

5.3 Configuration Roadmap for Oracle Access Management

Table 5–1 lists the tasks for configuring Oracle Access Management.

Table 5–1 Configuration Flow for Oracle Access Management

No.	Task	Description
1	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 5.4, "Configuring Oracle Access Management in a New WebLogic Domain".
2	Configure the Database Security Store.	For more information, see Section 5.5, "Configuring the Database Security Store.".
3	Start the Oracle WebLogic Administration Server.	For more information, see Section 5.6, "Starting the Oracle WebLogic Administration Server".
4	Complete the post-installation tasks.	Complete the following post-installation tasks: ■ Section 5.7, "Optional Post-Installation Tasks" ■ Section 5.8, "Optional: Configuring Oracle Mobile Security Suite" ■ Section 5.9, "Starting the Managed Servers" ■ Section 5.10, "Verifying the Oracle Access Management Installation" ■ Section 5.11, "Setting Up Oracle Access Manager Webgate Agents" ■ Section 5.12, "Setting Up Integration with OIM" ■ Section 5.13, "Getting Started with Oracle Access Management After Installation"

5.4 Configuring 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

5.4.1 Appropriate Deployment Environment

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

5.4.2 Components Deployed

Performing the configuration in this section deploys the following components:

- Oracle Access Manager
- Oracle Access Management Security Token Service
- Oracle Access Management Identity Federation
- Oracle Access Management Mobile and Social
- Oracle WebLogic Administration Server
- Managed Servers for Oracle Access Manager, Oracle Mobile Security Manager, and Oracle Access Manager Policy Manager.
- Oracle Access Management Console on the Administration Server
- Oracle Access Manager Policy Manager Console on the Policy Manager Managed Server

5.4.3 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 Access Manager and Oracle Mobile Security Manager. For more information, see Section 3.2.5, "Creating Database Schemas Using the Oracle Fusion Middleware Repository Creation Utility (RCU)".

5.4.4 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 Linux or 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 Mobile Security Suite.

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 And Mobile Security Suite - 11.1.2.3.0 [IAM_HOME]**, and click **Next**. The Specify Domain Name and Location screen appears.

   Note: When you select the **Oracle Access Management And Mobile Security Suite - 11.1.2.3.0 [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]**
   - **Oracle OPSS Metadata for JRF - 11.1.1.0 [oracle_common]**
   - **Oracle Enterprise Manager - 11.1.1.0 [oracle_common]**
   - **Oracle WSM Policy Manager - 11.1.1.0 [oracle_common]**

   If you are planning to configure Oracle Access Management Mobile and Social, 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.
4. Enter a name and a location for the domain to be created.

   For example,

   - **Domain name:** `oam_domain`
   - **Domain location:** *`ORACLE_BASE`*`/admin/oam/user_projects/domains`
   - **Application location:** *`ORACLE_BASE`*`/admin/oam/user_projects/applications`

   Notes:

   - *`ORACLE_BASE`* is the base directory under which Oracle products are installed. For example, `/u01/oracle`.
   - The default locations for the domain home and application home are *`MW_HOME`*`/user_projects/domains` and *`MW_HOME`*`/user_projects/applications`, respectively. However, it is recommended that you create your domain and application home directories outside of both the Middleware home and Oracle home.

   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 mode under **WebLogic Domain Startup Mode**. Click **Next**.

7. The Configure JDBC Component Schema screen appears. This screen displays a list of the following component schemas:

   - OAM MDS Schema
   - OWSM MDS Schema
   - OAM Infrastructure
   - OMSM Schema
   - OPSS Schema

   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.

   If the test fails, click **Previous**, correct the issue, and try again.

   After the test succeeds, click **Next**. The Select Optional Configuration screen appears.

8. On the Select Optional Configuration screen, select **Administration Server** and **Managed Servers, Clusters and Machines**.

   Click **Next**.

9. Use the Configure the Administration Server screen to configure the following Administration Server parameters:

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

   Click **Next**.

10. Configure Managed Servers.

    When you first enter the Configure Managed Servers screen, three default Managed Servers (`oam_server1`, `omsm_server1`, and `oam_policy_mgr1`) have been created for you and have been automatically assigned to default ports. Change the default Managed Server names to the following:

    - For the Oracle Access Manager Server entry (`oam_server1`), change the name to `WLS_OAM1`.
    - For the Oracle Mobile Security Manager Server entry (`omsm_server1`), change the name to `WLS_MSM1`.
    - For the Access Manager Policy Manager Server entry (`oam_policy_mgr1`), change the name to `WLS_AMA1`.

    These server names will be referenced throughout this document. If you choose different names, then be sure to replace them as needed.

Notes:

- If you want to configure the Managed Servers on the same machine as the Administration Server, ensure that the ports are different from that of the Administration Server. Modify the port numbers as needed.
- The Oracle Access Management OAuth Service is deployed on the Oracle Access Manager Server (`WLS_OAM1`). If you want to configure the OAuth Service in SSL mode, you must enable the SSL port of the Oracle Access Manager Server.
- For more information, see "Configure Managed Servers" in *Creating Domains Using the Configuration Wizard*.

Click **Next**.

11. On the Configure Clusters screen, click **Add** to create three clusters with the following names for Oracle Access Manager, Oracle Mobile Security Manager, and Oracle Access Manager Policy Manager:
    - `oam_cluster`
    - `msm_cluster`
    - `ama_cluster`

    Leave all other fields at the default settings and click **Next**.

    Note: 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 *High Availability Guide*.

12. On the Assign Servers to Clusters screen, assign Managed Servers to clusters as follows:
    - Assign the Oracle Access Manager Managed Server (**WLS_OAM1**) to **oam_cluster**.
    - Assign the Oracle Mobile Security Manager Managed Server (**WLS_MSM1**) to **msm_cluster**.
    - Assign the Policy Manager Managed Server (**WLS_AMA1**) to **ama_cluster.**

    Click **Next**.

13. Use the Configure Machines screen to create and configure machines in the domain, 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.

    Note: For more information about the options on this screen, see "Configure Machines" in *Creating Domains Using the Configuration Wizard*.

Note that if you are extending your domain over multiple machines, you should not migrate the domain to a remote machine until all configuration tasks are completed on the base machine (the machine on which the Administration Server is running).

Click **Next**.

14. On the Assign Servers to Machines screen, assign the Administration Server 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 Servers, such as `WLS_OAM1`, `WLS_MSM1`, and `WLS_AMA1`, to a machine.

    Click **Next**.

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

    By default, a new WebLogic domain to support Oracle Access Management is created in the *`MW_HOME`*`\user_projects\domains` directory.

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 *Administrator's Guide for Oracle Access Management*.

5.5 Configuring the Database Security Store

After configuring Oracle Access Management in a new WebLogic administration domain and before starting the Oracle WebLogic Administration Server, you must configure the Database Security Store by running the `configureSecurityStore.py` script. For more information, see Chapter 11, "Configuring Database Security Store for an Oracle Identity and Access Management Domain."

5.6 Starting the Oracle WebLogic Administration Server

After installing and configuring Oracle Access Management, you must start the Oracle WebLogic Administration Server, as described in Appendix C.1, "Starting the Stack". Ensure that you start the Oracle Access Management Administration Server before starting the Managed Servers.

5.7 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 *Administrator's Guide for Oracle Access Management*.

5.8 Optional: Configuring Oracle Mobile Security Suite

By default, Oracle Mobile Security Suite is installed (but not fully configured) with Oracle Access Management. To fully configure Oracle Mobile Security Suite with Oracle Access Management, follow the instructions in Chapter 10, "Configuring Oracle Mobile Security Suite."

5.9 Starting the Managed Servers

You must start the Managed Servers for Oracle Access Manager (`WLS_OAM1`), Access Manager Policy Manager (`WLS_AMA1`), and Oracle Mobile Security Manager (`WLS_MSM1`). For more information, see Appendix C.1, "Starting the Stack."

5.10 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 Servers are up and running.
2. Log in to the Administration Console for Oracle Access Management using the following 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. Log in to the Oracle Access Manager Policy Manager Console using the following URL:

   `http://oam_policy_mgr_host:oam_policy_mgr_port/access`

   When you access the Policy Manager Console running on the Policy Manager Server, you are prompted to enter a user name and password. Note that you must have Administrator's role and privileges.
4. Verify the Oracle WebLogic Server Administration Console. If the installation and configuration of Oracle Access Management are successful, this console shows the Administration Server in running mode.

5.11 Setting Up Oracle Access Manager Webgate Agents

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

5.12 Setting Up Integration with OIM

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

5.13 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 *Administrator's Guide for Oracle Access Managementt*.

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 *Administrator's Guide for Oracle Access Management*.

6

Configuring Oracle Adaptive Access Manager

This chapter explains how to configure Oracle Adaptive Access Manager.

It includes the following topics:

6.1 Overview

For Oracle Identity and Access Management 11*g* Release 2 (11.1.2.3.0), 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 (11.1.2.3.0), Oracle Adaptive Access Manager (Offline) is also installed along with Oracle Adaptive Access Manager. For configuring Oracle Adaptive Access Manager (Offline), see Section 6.5, "Configuring Oracle Adaptive Access Manager (Offline)".

6.2 Important Note Before You Begin

Before you start configuring Oracle Adaptive Access Manager, 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 Privileged Account Manager, Oracle Access Management Mobile and

Social, and Oracle Mobile Security Suite. You can specify any path for this Oracle Home directory.

6.3 Configuration Roadmap for Oracle Adaptive Access Manager

Table 6–1 lists the tasks for configuring Oracle Adaptive Access Manager.

Table 6–1 Configuration Flow for Oracle Adaptive Access Manager

No.	Task	Description
1	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 6.4, "Oracle Adaptive Access Manager in a New WebLogic Domain" ■ Section 6.5, "Configuring Oracle Adaptive Access Manager (Offline)"
2	Configure the Database Security Store.	For more information, see Section 6.6, "Configuring the Database Security Store."
3	Start the servers.	You must start the Administration Server and all Managed Servers. For more information, see Section 6.7, "Starting the Servers".
4	Complete the post-installation tasks.	Complete the following post-installation tasks: ■ Section 6.8, "Post-Installation Steps" ■ Section 6.9, "Verifying the Oracle Adaptive Access Manager Installation" ■ Section 6.10, "Getting Started with Oracle Adaptive Access Manager After Installation"

6.4 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

6.4.1 Appropriate Deployment Environment

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

6.4.2 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.

6.4.3 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 3.2.5, "Creating Database Schemas Using the Oracle Fusion Middleware Repository Creation Utility (RCU)".

6.4.4 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 Linux or 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 Mobile Security Suite.

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]**
   - **Oracle OPSS Metadata for 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, **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.

   Note: The default locations for the domain home and application home are *MW_HOME*/user_projects/domains and *MW_HOME*/user_projects/applications, respectively. However, it is recommended that you create your domain and application home directories outside of both the Middleware home and Oracle home.

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 mode under **WebLogic Domain Startup Mode**. Click **Next**.
7. On the Configure JDBC Component Schema screen, select a component schema, such as the **OAAM Admin 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.

   If the test fails, click **Previous**, correct the issue, and try again.

   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 and Machines**, **Deployments and Services,** and **RDBMS Security Store**. Select the relevant check boxes 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.

    Note: For more information, see "Configure Managed Servers" in *Creating Domains Using the Configuration Wizard*.

11. Optional: Configure Clusters, as required.

    Note: For more information about configuring clusters for Oracle Identity and Access Management components, see the "Configuring High Availability for Oracle Identity and Access Management Components" topic in the *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: Assign the newly created Managed Servers to a machine.
16. Optional: Select Deployments, such as applications and libraries, and Services to target them to a particular cluster or server.
17. Optional: Configure RDBMS Security Store, as required.
18. On the Configuration Summary screen, review the domain configuration, and click **Create** to start creating the domain.

By default, a new WebLogic domain to support Oracle Adaptive Access Manager is created in the *MW_HOME*`\user_projects\domains` directory (on Windows). On Linux or UNIX, the domain is created in the *MW_HOME*`/user_projects/domains` directory, by default.

6.5 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

6.5.1 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

6.5.2 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 3.2.5, "Creating Database Schemas Using the Oracle Fusion Middleware Repository Creation Utility (RCU)".

6.5.3 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 Linux or 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]**
   - **Oracle OPSS Metadata for 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.

   If the test fails, click **Previous**, correct the issue, and try again.

   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.
- 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 *High Availability Guide*.

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

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

- Optional: Assign the Administration Server to a machine.
- Optional: Assign the newly created Managed 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.

By default, a new WebLogic domain to support Oracle Adaptive Access Manager (Offline) is created in the *MW_HOME*`\user_projects\domains` directory (on Windows). On Linux or UNIX, the domain is created in the *MW_HOME*`/user_projects/domains` directory, by default.

6.6 Configuring the Database Security Store

After configuring Oracle Adaptive Access Manager in a new WebLogic administration domain and before starting the Oracle WebLogic Administration Server, you must configure the Database Security Store by running the `configureSecurityStore.py` script. For more information, see Chapter 11, "Configuring Database Security Store for an Oracle Identity and Access Management Domain."

6.7 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.

6.8 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 **Security Realms**, and then click 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 *Administering 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 recreate 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 *`IAM_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 *`IAM_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 *`IAM_HOME`*`/oaam/init` directory.
- Configurable action templates are shipped in the `OOTB_Configurable_Actions.zip` file, which is located in the *`IAM_HOME`*`/oaam/init` directory.
- Base-authentication required entities are shipped in the `Auth_EntityDefinition.zip` file, which is located in the *`IAM_HOME`*`/oaam/init` directory.

Note: For more information about policies, see "Importing the OAAM Snapshot" and "Managing Policies, Rules, and Conditions" topics in *Administering 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 *Administering Oracle Adaptive Access Manager*.

   b. Make a copy of the `sample.bharosa_location.properties` file, which is located under the *`IAM_HOME`*`/oaam/cli` directory (on Linux or UNIX). On Windows, the `sample.bharosa_location.properties` file is located under the *`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 Linux or 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 Linux or 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*.

6.9 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:

     DOMAIN_HOME`\bin\startWebLogic`
   - On Linux or UNIX: At the $ prompt, run the `startWebLogic.sh` script to start the Administration Server, as in the following example:

     DOMAIN_HOME`/bin/startWebLogic.sh`
2. Start the Managed Servers, as described in Appendix C.1, "Starting the Stack.".

   Wait for the Administration Server and the Managed Servers 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
```

6.10 Getting Started with Oracle Adaptive Access Manager After Installation

After installing Oracle Adaptive Access Manager, refer to *Administering Oracle Adaptive Access Manager*.

7

Configuring Oracle Entitlements Server

This chapter describes how to configure Oracle Entitlements Server 11*g* Release 2 (11.1.2.3.0).

It discusses the following topics:

- Important Note Before You Begin
- Overview of Oracle Entitlements Server 11g Installation
- 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

7.1 Important Note Before You Begin

Before you start 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 Privileged Account Manager, Oracle Access Management Mobile and Social, and Oracle Mobile Security Suite. You can specify any path for this Oracle Home directory.

7.2 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 *Administering 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 (11.1.2.3.0) 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 (11.1.2.3.0) installation. The Oracle Entitlements Server Client does not require Oracle WebLogic Server.

7.3 Configuration Roadmap for Oracle Entitlements Server

Table 7–1 lists the tasks for configuring Oracle Entitlements Server.

Table 7–1 Configuration Flow for Oracle Entitlements Server

No.	Task	Description
1	Run the Oracle Fusion Middleware Configuration Wizard to configure Oracle Entitlements Server Administration Server.	For more information, see Section 7.4, "Configuring Oracle Entitlements Server Administration Server".
2	Install the Oracle Entitlements Server Client software.	For more information, see Section 7.5, "Installing Oracle Entitlements Server Client".
3	Configure Oracle Entitlements Server Client.	For more information, see Section 7.6, "Configuring Oracle Entitlements Server Client".
4	Get started with Oracle Entitlements Server.	For more information, see Section 7.7, "Getting Started with Oracle Entitlements Server After Installation".

7.4 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
- Configuring SSL When Configuring the Database Security Store
- Configuring the Database Security Store for Oracle Entitlements Server Administration Server
- Starting the Servers
- Verifying Oracle Entitlements Server Configuration

7.4.1 Components Deployed

Performing the configuration in this section deploys the following:

- WebLogic Administration Server
- Oracle Entitlements Server application on the Administration Server

7.4.2 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`

7.4.3 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 Linux or 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 Mobile Security Suite.

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]**
  - **Oracle OPSS Metadata for 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]**
  - **Oracle OPSS Metadata for JRF 11.1.1.0 [oracle_common]**
- If you are using Apache Derby, then select the **Oracle Entitlements Server Derby Template - 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.

Note: The default locations for the domain home and application home are *MW_HOME*/user_projects/domains and *MW_HOME*/user_projects/applications, respectively. However, it is recommended that you create your domain and application home directories outside of both the Middleware home and Oracle home.

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 mode under **WebLogic Domain Startup Mode**. Click **Next**.

   The Configure JDBC Component Schema screen is displayed.

7. On the Configure JDBC Component Schema screen, select the **OPSS 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.

By default, a new WebLogic domain to support Oracle Entitlements Server is created in the *MW_HOME*`\user_projects\domains` directory (on Windows). On Linux or UNIX, the domain is created in the *MW_HOME*`/user_projects/domains` directory, by default.

7.4.4 Configuring SSL When Configuring the Database Security Store

After you have created the appropriate database schemas and have configured Oracle Entitlements Server in a WebLogic domain, you can configure SSL when configuring the database security store. To configure the database security store, you must run the `configureSecuritystore.py` script. To configure SSL when configuring the database security store, you must complete the following steps before running the `configureSecuritystore.py` script.

Notes:

- It is assumed that, at this point, the database is properly configured with SSL, and the Keystore and Truststore are already created using the command `keytool`.
- In the following steps, the property `oracle.net.ssl_version=1.0` is set for a database server that is configured to use Transport Layer Security (TLS) version 1.0. If the database server does not use TLS 1.0, then you must set the property `oracle.net.ssl_version` to the corresponding value. This property is used to set the SSL version that the JDBC driver uses. The value specified should be supported by both SSL and the server.
- For more information on running the `configureSecuritystore.py` script, see Section 7.4.5, "Configuring the Database Security Store for Oracle Entitlements Server Administration Server".

1. Update the Database URL in the JDBC configuration file `opss-jdbc.xml` by doing the following:

   a. Open the *DOMAIN_HOME*`/config/jdbc/opss-jdbc.xml` file for editing.

   The `opss-jdbc.xml` file contains schema and database server information for Oracle Entitlements Server and Oracle Platform Security Services.

   b. Edit the Database URL to change it from:

   `jdbc:oracle:thin:@`*db_host:db_port/service_name*

   to

   `jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCPS)(HOST=`*db_hostname*`)(PORT=`*db_port_number*`)))(CONNECT_DATA=(SERVER=DEDICATED)(SERVICE_NAME=`*db_service_name*`)))`

   c. Add the following properties:

```
<property>
<name>javax.net.ssl.keyStore</name>
<value>path_to_keystore</value>
</property>
<property>
<name>javax.net.ssl.keyStorePassword</name>
<value>keystore_password</value>
</property>
<property>
<name>javax.net.ssl.trustStore</name>
<value>path_to_truststore</value>
</property>
<property>
<name>javax.net.ssl.trustStorePassword</name>
<value>truststore_password</value>
</property>
<property>
<name>oracle.net.ssl_version</name>
<value>TLS_version</value>
</property>
```

Where,

path_to_keystore refers to the absolute path to the keystore. For example, /home/certs/dbcerts/mycerts/keystore.jks.

keystore_password refers to the password of the key store.

path_to_truststore refers to the absolute path to the truststore. For example, /home/certs/dbcerts/mycerts/truststore.jks.

truststore_password refers to the password of the truststore.

TLS_version refers to the Transport Layer Security (TLS) version. If the database server is configured to use the TLS version 1.0, you must specify 1.0.

d. Save the file and exit.

2. Edit the WLST script by doing the following:

a. Open the *MW_HOME*/wlserver_10.3/common/bin/wlst.sh file for editing.

b. Update the following line:

```
JVM_ARGS="-Dprod.props.file='${WL_HOME}'/.product.properties
${WLST_PROPERTIES} ${JVM_D64} ${MEM_ARGS} ${CONFIG_JVM_ARGS}"
```

to change it to

```
JVM_ARGS="-Dprod.props.file='${WL_HOME}'/.product.properties
${WLST_PROPERTIES} ${JVM_D64} ${MEM_ARGS} ${CONFIG_JVM_ARGS}
-Djavax.net.ssl.trustStorePassword=trust_store_password
-Djavax.net.ssl.keyStorePassword=key_store_password
-Djavax.net.ssl.keyStore=path_to_keystore
-Djavax.net.ssl.trustStore=path_to_truststore -Doracle.net.ssl_
version=TLS_version"
```

For example:

```
JVM_ARGS="-Dprod.props.file='${WL_HOME}'/.product.properties ${WLST_
PROPERTIES} ${JVM_D64} ${MEM_ARGS} ${CONFIG_JVM_ARGS}
-Djavax.net.ssl.trustStorePassword=welcome1
-Djavax.net.ssl.keyStorePassword=welcome2
-Djavax.net.ssl.keyStore=/home/certs/dbcerts/mycerts/keystore.jks
-Djavax.net.ssl.trustStore=/home/certs/dbcerts/mycerts/truststore.jks
-Doracle.net.ssl_version=1.0"
```

In the above example, the property "-Doracle.net.ssl_version=1.0" represents that the database server is configured to use the Transport Layer Security (TLS) version 1.0.

c. Save the file and exit.

3. Edit the configureSecurityStore.py script by doing the following:

a. Open the *MW_HOME*/*IAM_HOME*/common/tools/configureSecurityStore.py file for editing.

b. Edit the following line to change it from:

```
full_command_parts = ("java -Doracle.security.jps.config=",
escapedJpsConfPath, "
oracle.security.jps.internal.api.credstore.CredstoreUtil",
```

to

```
full_command_parts = ("java
-Djavax.net.ssl.trustStorePassword=truststore_password
-Djavax.net.ssl.keyStorePassword=keystore_password
-Djavax.net.ssl.keyStore=path_to_keystore
-Djavax.net.ssl.trustStore=path_to_truststore -Doracle.net.ssl_
version=TLS_version -Doracle.security.jps.config=",
escapedJpsConfPath, "
oracle.security.jps.internal.api.credstore.CredstoreUtil",
```

For example:

```
full_command_parts = ("java -Djavax.net.ssl.trustStorePassword=welcome1
-Djavax.net.ssl.keyStorePassword=welcome2
-Djavax.net.ssl.keyStore=/home/certs/dbcerts/mycerts/keystore.jks
-Djavax.net.ssl.trustStore=/home/certs/dbcerts/mycerts/truststore.jks
-Doracle.net.ssl_version=1.0
-Doracle.security.jps.config=", escapedJpsConfPath, "
oracle.security.jps.internal.api.credstore.CredstoreUtil",
```

c. The following line occurs twice. Edit the line to change it from:

```
full_command_parts = ("java -Xms512M -Xmx512M ",
"oracle.security.jps.internal.tools.configuration.ldap.LdapServiceE
nabler ", command)
```

to

```
full_command_parts = ("java -Xms512M -Xmx512M
-Djavax.net.ssl.trustStorePassword=truststore_password
-Djavax.net.ssl.keyStorePassword=keystore_password
-Djavax.net.ssl.keyStore=path_to_keystore
-Djavax.net.ssl.trustStore=path_to_truststore -Doracle.net.ssl_
version=TLS_version ",
"oracle.security.jps.internal.tools.configuration.ldap.LdapServiceE
nabler ", command)
```

For example:

```
full_command_parts = ("java -Xms512M -Xmx512M
-Djavax.net.ssl.trustStorePassword=welcome1
-Djavax.net.ssl.keyStorePassword=welcome2
-Djavax.net.ssl.keyStore=/home/certs/dbcerts/mycerts/keystore.jks
-Djavax.net.ssl.trustStore=/home/certs/dbcerts/mycerts/truststore.jks
-Doracle.net.ssl_version=1.0 ",
"oracle.security.jps.internal.tools.configuration.ldap.LdapServiceEnabler
", command)
```

d. Save the `configureSecurityStore.py` script and exit.

4. Edit the `startWebLogic` script by doing the following:

a. Open the *DOMAIN_HOME*`/bin/startWebLogic.sh` file for editing.

b. Edit the following line to change it from:

```
JAVA_OPTIONS="${JAVA_OPTIONS} -Dlaunch.main.class=${SERVER_CLASS}
-Dlaunch.class.path="${CLASSPATH}"
-Dlaunch.complete=weblogic.store.internal.LockManagerImpl -cp ${WL_
HOME}/server/lib/pcl2.jar"
```

to

```
JAVA_OPTIONS="${JAVA_OPTIONS}
-Djavax.net.ssl.trustStorePassword=truststore_password
-Djavax.net.ssl.keyStorePassword=keystore_password
-Djavax.net.ssl.keyStore=path_to_keystore
-Djavax.net.ssl.trustStore=path_to_truststore -Doracle.net.ssl_
version=TLS_version -Dlaunch.main.class=${SERVER_CLASS}
-Dlaunch.class.path="${CLASSPATH}"
-Dlaunch.complete=weblogic.store.internal.LockManagerImpl -cp ${WL_
HOME}/server/lib/pcl2.jar"
```

For example:

```
JAVA_OPTIONS="${JAVA_OPTIONS} -Djavax.net.ssl.trustStorePassword=welcome1
-Djavax.net.ssl.keyStorePassword=welcome2
-Djavax.net.ssl.keyStore=/home/certs/dbcerts/mycerts/keystore.jks
-Djavax.net.ssl.trustStore=/home/certs/dbcerts/mycerts/truststore.jks
-Doracle.net.ssl_version=1.0 -Dlaunch.main.class=${SERVER_CLASS}
-Dlaunch.class.path="${CLASSPATH}"
-Dlaunch.complete=weblogic.store.internal.LockManagerImpl -cp ${WL_
HOME}/server/lib/pcl2.jar"
```

c. Save the file and exit.

Note: If you have Managed Server, you must update the script *OES_DOMAIN_HOME*/bin/startManagedWebLogic.sh as described for startWebLogic.sh script.

---

5. Configure the database security store by running the configureSecurityStore.py script. For more information, see Section 7.4.5, "Configuring the Database Security Store for Oracle Entitlements Server Administration Server".

   After you configure the database security store, start the domain. Then, you can verify that it uses database SSL connection.

7.4.5 Configuring the Database Security Store for Oracle Entitlements Server Administration Server

You must run the configureSecurityStore.py script to configure the Database 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.

Note: If you want to configure SSL when configuring the database security store, then you must complete the steps in Section 7.4.4, "Configuring SSL When Configuring the Database Security Store" before running the configureSecuritystore.py 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 DOMAIN_HOME -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 Linux or UNIX:

```
MW_HOME/oracle_common/common/bin/wlst.sh IAM_
HOME/common/tools/configureSecurityStore.py -d DOMAIN_HOME -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 7–2 describes the parameters that you may specify on the command line.

Table 7–2 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 7–2 (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.

7.4.6 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.

7.4.7 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 *`DOMAIN_HOME`*`/servers/AdminServer/logs` directory (on Linux or UNIX) or the *`DOMAIN_HOME`*`\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 *Administering Oracle Entitlements Server*.

7.5 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

7.5.1 Prerequisites

Before installing the Oracle Entitlements Server Client software, ensure that you have installed and configured the Oracle Entitlements Server Administration Server.

7.5.2 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*.

7.5.3 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:

Linux or 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 7–3 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 7–3 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 7–3 (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 Linux or UNIX system, you may be asked to run the *OES_CLIENT_HOME/oracleRoot.sh* script to set up the proper file and directory permissions.
6	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.

7.5.4 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.

7.6 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

7.6.1 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

7.6.1.1 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 7–4.

Table 7–4 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.

7.6.1.2 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 7–5.

Table 7–5 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`.

7.6.1.2.1 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. The data source should be created in the domain where the Security Module instance is deployed. 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 the *DOMAIN_HOME*`/config/fmwconfig/` directory (on Linux or UNIX) or the *DOMAIN_HOME*`\config\fmwconfig\` directory (on Windows). *DOMAIN_HOME* is the domain location of the Oracle Entitlements Server Administration Server.

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. 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. The data source should be created in the domain where the Security Module instance is deployed. 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 *DOMAIN_HOME*`/config/fmwconfig` directory (on Linux or UNIX) or *DOMAIN_HOME*`\config\fmwconfig` directory (on Windows). *DOMAIN_HOME* is the domain location of the Oracle Entitlements Server Administration Server.

      `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".

7.6.2 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

7.6.2.1 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 7–4.
2. Run the `config.sh` (located in *`OES_CLIENT_HOME`*`/oessm/bin` on Linux or 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)

7.6.2.2 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 7–4.
2. Run the `config.sh` (located in `OES_CLIENT_HOME/oessm/bin` on Linux or 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)

7.6.2.3 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 7–4.
2. Run the `config.sh` (located in `OES_CLIENT_HOME/oessm/bin` on Linux or 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)

7.6.2.4 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 7–4.
2. Run the `config.sh` (located in `OES_CLIENT_HOME/oessm/bin` on Linux or 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.

7.6.3 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

7.6.3.1 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 Linux or UNIX) or `config.cmd` (located in *`OES_CLIENT_HOME`*`\oessm\bin` on Windows) as follows:

On Linux or 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 7–6 describes the parameters you specify on the command line.

Table 7–6 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 7.6.1.2, "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

7.6.3.1.1 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**.

   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".

7.6.3.1.2 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**.

   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".

7.6.3.2 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 Linux or 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 7–7 describes the parameters you specify on the command line.

Table 7–7 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 7.6.1.2, "Configuring Non-Controlled and Controlled Pull Distribution Mode".

This command also creates client configuration for Webservice Security Module Instance.

7.6.3.3 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 Linux or 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 7–8 describes the parameters you specify on the command line.

Table 7–8 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.
`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`

Table 7–8 (Cont.) Parameters for Web Service Security Module on Oracle WebLogic

Parameters	Description
`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 7.6.1.2, "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

7.6.3.3.1 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**.

   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".

7.6.3.3.2 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**.

   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".

7.6.3.4 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 Linux or 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 7–9 Oracle Service Bus Security Module Parameters

Parameter	Description
`smType`	Type of security module instance you want to create. For example, `jboss`.

Table 7–9 (Cont.) Oracle Service Bus Security Module Parameters

Parameter	Description
`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**.

   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

7.6.3.5 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*.

7.6.3.6 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 Linux or 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 7–10 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 7.6.1.2, "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**.

7.6.3.7 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 Linux or 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_ssl_port -sslPort tomcat_server_ssl_port
-serverLocation apache-tomcat Home -jaxwsRIHome  jaxwsRI_Home  -serverUserName
username -serverPassword password
```

Table 7–11 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 SSL port number of the Oracle Entitlements Server Administration Server. For example, `7002`.
`sslPort`	The SSL port number of the Apache Tomcat Server. For example, `8449`.
`serverLocation`	The location of Apache Tomcat Server.

Table 7–11 (Cont.) Apache Tomcat Security Module Parameters

Parameter	Description
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 7.6.1.2, "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**.

7.6.3.8 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 Linux or 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 7–12 describes the parameters you specify on the command line.

Table 7–12 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 7.6.1.2, "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 7–12.

7.6.3.9 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 Linux or 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 7–13 describes the parameters you specify on the command line.

Table 7–13 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 7.6.1.2, "Configuring Non-Controlled and Controlled Pull Distribution Mode".

This command also creates client configuration for the RMI Security Module Instance.

7.6.3.10 Configuring Microsoft .NET Security Module

This section includes the following topics:

- Prerequisites for Configuring .NET Security Module
- Microsoft .NET Configuration Scenarios

7.6.3.10.1 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`.

7.6.3.10.2 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 7–14 describes the parameters you specify on the command line.

Table 7–14 .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`.

Table 7–14 (Cont.) .NET Security Module Parameters

Parameter	Description
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 7–16 describes the parameters you specify on the command line.

Table 7–15 .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 7–16 describes the parameters you specify on the command line.

Table 7–16 .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>
```

7.6.3.11 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

7.6.3.11.1 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.

7.6.3.11.2 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 7–17 describes the parameters you specify on the command line.

Table 7–17 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 7–19 describes the parameters you specify on the command line.

Table 7–18 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 7–19 describes the parameters you specify on the command line.

Table 7–19 MOSS Security Module Parameters

Parameter	Description
`smType`	The type of security module instance you want to create. For example, `moss`.

Table 7–19 (Cont.) MOSS Security Module Parameters

Parameter	Description
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.

7.6.3.11.3 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
```

7.6.3.11.4 Migrating Resource Policies

To migrate the MOSS resource policies to OES policy store, complete the following steps:

1. Create an empty file named `jps-config.xml` in the directory of your choice. Then, open up the file and add the following content:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<jpsConfig xmlns="http://xmlns.oracle.com/oracleas/schema/11/jps-config-11_
1.xsd">
    <serviceProviders>
        <serviceProvider type="POLICY_STORE" name="policy.db"
class="oracle.security.jps.internal.policystore.OPSSPolicyStoreProvider" />
    </serviceProviders>
    <serviceInstances>
        <serviceInstance name="policystore.db" provider="policy.db">
            <property name="policystore.type" value="DB_ORACLE" />
            <property name="jdbc.url" value="jdbc:oracle:thin:@db_host:db_
port:service_name" />
            <property name="jdbc.driver"
value="oracle.jdbc.driver.OracleDriver" />
            <property name="security.principal" value="prefix_OPSS" />
            <property name="security.credential" value="password" />
            <property name="oracle.security.jps.farm.name" value="cn=oes_
domain"/>
            <property name="oracle.security.jps.ldap.root.name"
value="cn=jpsroot" />
        </serviceInstance>
    </serviceInstances>
    <jpsContexts default="default">
        <jpsContext name="default">
            <serviceInstanceRef ref="policystore.db" />
        </jpsContext>
    </jpsContexts>
</jpsConfig>
```

2. Go to `OES_CLIENT_HOME/oessm/bin` directory (on Windows), or `OES_CLIENT_HOME\oessm\bin` directory (on Linux or UNIX)

3. Update the variable `-Doracle.security.jps.config` in `manage-policy.cmd` (on Windows) or in `manage-policy.sh` (on Linux or UNIX) so that `-Doracle.security.jps.config` points to the `jps-config.xml` file you created in step 1.
4. Update the `OES_CLIENT_HOME` and `OES_INSTANCE_NAME` variables in `manage-policy.cmd` (on Windows) or in `manage-policy.sh` (on Linux or UNIX) to reflect your Oracle Entitlements Server Client environment.
5. Run the `manage-policy.cmd` file (on Windows) or `manage-policy.sh` file (on Linux or 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
```

7.6.4 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.

7.6.5 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 Linux or 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.

7.6.6 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 7–20:

Table 7–20 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 Linux or 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 E, "Configuring the PDP Proxy Client for Web Service Security Module".

7.7 Getting Started with Oracle Entitlements Server After Installation

After installing Oracle Entitlements Server, refer to the following documents:

- *Administering Oracle Entitlements Server*
- *Developer's Guide for Oracle Entitlements Server*

8

Configuring Oracle Privileged Account Manager

This chapter explains how to configure Oracle Privileged Account Manager.

It includes the following topics:

8.1 Overview

For an introduction to the Oracle Privileged Account Manager, see "Understanding Oracle Privileged Account Manager" in *Administering Oracle Privileged Account Manager*.

8.2 Important Note Before You Begin

Before you start configuring Oracle Privileged Account Manager, 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 Privileged Account Manager, Oracle Access Management Mobile and Social, and Oracle Mobile Security Suite. You can specify any path for this Oracle Home directory.

8.3 Configuration Roadmap for Oracle Privileged Account Manager

Table 8–1 lists the tasks for configuring Oracle Privileged Account Manager.

Table 8–1 Configuration Flow for Oracle Privileged Account Manager

No.	Task	Description
1	Optional: Enable TDE in OPAM data store.	For more information, see Section 8.4, "Optional: Enabling TDE in Oracle Privileged Account Manager Data Store"
2	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 8.5, "Configuring Oracle Privileged Account Manager in a New WebLogic Domain".
3	Configure the Database Security Store.	For more information, see Section 8.6, "Configuring the Database Security Store."
4	Complete the post-installation tasks.	Complete the following post-installation tasks: ■ Section 8.7, "Starting the Oracle WebLogic Administration Server" ■ Section 8.8, "Post-Installation Tasks" ■ Section 8.9, "Starting the Managed Server" ■ Section 8.10, "Assigning the Application Configurator Role to a User" ■ Section 8.11, "Optional: Setting Up Non-TDE Mode" ■ Section 8.12, "Optional: Configuring OPAM Console" ■ Section 8.13, "Verifying Oracle Privileged Account Manager" ■ Section 8.14, "Getting Started with Oracle Privileged Account Manager After Installation"

8.4 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

8.4.1 Enabling TDE in the Database

For information about enabling Transparent Data Encryption (TDE) in the database for Oracle Privileged Account Manager, refer to one of the following procedures, depending on the Oracle Database version you are using:

- To enable TDE in Oracle Database Release 11.2, refer to the "Enabling Transparent Data Encryption" topic in the *Oracle Database Advanced Security Administrator's Guide*.
- To enable TDE in Oracle Database Release 12.1, refer to the "Configuring Transparent Data Encryption" topic in the *Oracle Database Advanced Security 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 8.4.2, "Enabling Encryption in OPAM Schema".

8.4.2 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
```

8.5 Configuring Oracle Privileged Account Manager in a New WebLogic Domain

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

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure

8.5.1 Appropriate Deployment Environment

Perform the configuration in this topic if you want to configure Oracle Privileged Account Manager in a new WebLogic domain.

8.5.2 Components Deployed

Performing the configuration in this section deploys Oracle Privileged Account Manager on a new WebLogic domain.

8.5.3 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 3.2.5, "Creating Database Schemas Using the Oracle Fusion Middleware Repository Creation Utility (RCU)".

8.5.4 Procedure

Perform the following steps to configure Oracle Privileged Account 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 Linux or 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 Mobile Security Suite.

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 Platform Security Service 11.1.1.0 [IAM_HOME]**
   > - **Oracle JRF 11.1.1.0 [oracle_common]**
   > - **Oracle OPSS Metadata for 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.

   > **Note:** The default locations for the domain home and application home are *MW_HOME*/user_projects/domains and *MW_HOME*/user_projects/applications, respectively. However, it is recommended that you create your domain and application home directories outside of both the Middleware home and Oracle home.

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 mode under **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.

If the test fails, click **Previous**, correct the issue, and try again.

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.

    Note: The default Managed Server name where Oracle Privileged Account Manager is deployed is `opam_server1`.

    For more information, see "Configure Managed Servers" in *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 *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: Assign the Managed Server to a machine.
16. Optional: Select Deployments, such as applications and libraries, and Services to target them to a particular cluster or server.
17. Optional: Configure RDBMS Security Store, as required.
18. On the Configuration Summary screen, you can view summaries of your configuration for deployments, application, and service. Review the domain configuration, and click **Create** to start creating the domain.

By default, a new WebLogic domain to support Oracle Privileged Account Manager is created in the *MW_HOME*\user_projects\domains directory (on Windows). On Linux or UNIX, the domain is created in the *MW_HOME*/user_projects/domains directory, by default.

8.6 Configuring the Database Security Store

After configuring Oracle Privileged Account Manager in a new WebLogic administration domain and before starting the Oracle WebLogic Administration Server, you must configure the Database Security Store by running the configureSecurityStore.py script. For more information, see Chapter 11, "Configuring Database Security Store for an Oracle Identity and Access Management Domain."

8.7 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".

8.8 Post-Installation Tasks

After installing and configuring Oracle Privileged Account Manager, you must run the opam-config.sh script (on Linux or 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 Linux or 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 **Linux or 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 Linux or UNIX) or `opam-config.bat` script (on Windows). Provide the following information, when prompted:
  - Oracle WebLogic Administration user name
  - 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 *`DOMAIN_HOME/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 Linux or 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".

8.9 Starting the Managed Server

You must start the Oracle Privileged Account Manager Managed Server, as described in Appendix C.1, "Starting the Stack".

8.10 Assigning the Application Configurator Role to a User

After you complete the installation process, you do not have any users present with administrator roles. You must select a user and grant that user the *Application Configurator* role.

Note: For more information, see "Assigning the Application Configurator Role to a User" in *Administering Oracle Privileged Account Manager*.

For information about the Administration Roles that the Application Configurator user can have, see "Administration Role Types" in *Administering Oracle Privileged Account Manager*.

8.11 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 8.4, "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 **Linux or 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 *Administering Oracle Privileged Account Manager*.

8.12 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.

8.13 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 user name 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 are successful, this console shows `opam_server1` ,which is the default Managed Server, in running mode.

4. In the Domain Structure pane, click **Deployments**. The following applications should be listed in the Deployments table, and the state must be `Active`:

   - `oinav`
   - `opam`
   - `opamsessionmgr`

8.14 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 *Administering Oracle Privileged Account Manager*.

9

Configuring Oracle Access Management Mobile and Social

This chapter explains how to configure Oracle Access Management Mobile and Social.

It includes the following topics:

9.1 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.

Perform the configuration described in this chapter 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.

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

9.2 Important Note Before You Begin

Before you start configuring Oracle Access Management Mobile and Social, 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 Privileged Account Manager, Oracle Access Management Mobile and Social, and Oracle Mobile Security Suite. You can specify any path for this Oracle Home directory.

9.3 Configuration Roadmap for Oracle Access Management Mobile and Social

Table 9–1 lists the tasks for configuring Oracle Access Management Mobile and Social.

Table 9–1 Configuration Flow for Oracle Access Management Mobile and Social

No.	Task	Description
1	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 9.4, "Configuring Oracle Access Management Mobile and Social with Oracle Access Manager"
2	Configure the Database Security Store.	For more information, see Section 9.5, "Configuring the Database Security Store." **Note:** If you are configuring Oracle Access Management Mobile and Social standalone, skip this step.
3	Start the servers.	You must start the Administration Server and all Managed Servers. For more information, see Section 9.6, "Starting the Servers."
4	Complete the post-installation tasks.	Complete the following post-installation tasks: ■ Section 9.7, "Verifying Oracle Access Management Mobile and Social" ■ Section 9.8, "Getting Started with Oracle Access Management Mobile and Social After Installation"

9.4 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. To configure Oracle Access Management Mobile and Social and Oracle Access Manager in a new WebLogic administration domain, follow the instructions in Section 5.4, "Configuring Oracle Access Management in a New WebLogic Domain."

9.5 Configuring the Database Security Store

After configuring Oracle Access Management Mobile and Social with Oracle Access Management in a new WebLogic administration domain and before starting the Oracle WebLogic Administration Server, you must configure the Database Security Store by running the `configureSecurityStore.py` script. For more information, see Chapter 11, "Configuring Database Security Store for an Oracle Identity and Access Management Domain.".

9.6 Starting the Servers

After installing and configuring Oracle Access Management Mobile and Social with Oracle Access Management, you must start 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.

9.7 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, click the **Configuration** tab in the top right corner, and then click **Available Services**.

   The **Available Services** page opens.

   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.

9.8 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 *Administrator's Guide for Oracle Access Management*.

10

Configuring Oracle Mobile Security Suite

This chapter explains how to configure Oracle Mobile Security Suite. It includes the following topics:

10.1 Overview

For Oracle Identity and Access Management 11*g* Release 2 (11.1.2.3.0), Oracle Mobile Security Suite includes the following components:

- Oracle Mobile Security Manager
- Oracle Mobile Security Access Server

> **Note:** Oracle Mobile Security Manager is included in the Oracle Identity and Access Management Suite. When you are installing Oracle Identity and Access Management 11*g* Release 2 (11.1.2.3.0), only Oracle Mobile Security Manager is installed. Oracle Mobile Security Access Server has its own installer, and it is not included in the Oracle Identity and Access Management 11*g* Release 2 (11.1.2.3.0) installation. You must install and configure Mobile Security Manager before installing Mobile Security Access Server. For more information on installing Mobile Security Access Server, see Section 10.12, "Installing Oracle Mobile Security Access Server."

For an introduction to Oracle Mobile Security Suite, see "Understanding Oracle Mobile Security Suite" in *Administering Oracle Mobile Security Suite*.

10.2 Important Note Before You Begin

Before you start configuring Oracle Mobile Security Suite, 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 Privileged Account Manager, Oracle Access Management Mobile and Social, and Oracle Mobile Security Suite. You can specify any path for this Oracle Home directory.

10.3 Configuration Roadmap for Oracle Mobile Security Suite

Table 10–1 lists the tasks for configuring Oracle Mobile Security Suite.

Table 10–1 Configuration Flow for Oracle Mobile Security Suite

No.	Task	Description
1	Configure Oracle Access Management in a WebLogic domain.	For more information, see Section 10.4, "Configuring Oracle Access Management in a WebLogic Domain.".
2	Prepare your LDAP directory to be used as the common identity store for Oracle WebLogic Server, Oracle Access Manager, and Oracle Mobile Security Suite.	For more information, see Section 10.6, "Preparing Your LDAP Directory as the Identity Store"
3	Configure the Oracle Access Manager Server that will be used with Oracle Mobile Security Suite.	You configure Oracle Access Manager using the `idmConfigTool` command. For more information, see Section 10.7, "Configuring Oracle Access Manager for Oracle Mobile Security Suite."
4	Configure the identity store, keystores, and trust stores for the Oracle Mobile Security Manager Server.	You configure Oracle Mobile Security Manager using the `idmConfigTool` command. For more information, see Section 10.8, "Configuring Oracle Mobile Security Manager."
5	Start the Managed Servers.	For more information, see Section 10.9, "Starting the Managed Servers."
6	Verify your configuration.	Ensure Oracle Mobile Security Suite is enabled on the Policy Manager Console. For more information, see Section 10.10, "Verifying Oracle Access Manager and Oracle Mobile Security Manager."
7	Optional: Create and add additional administrator groups after configuration.	For more information, see Section 10.11, "Optional: Creating Additional Administrator Groups After Configuration."
8	Install and configure the Oracle Mobile Security Access Server software.	For more information, see Section 10.12, "Installing Oracle Mobile Security Access Server."
9	Get started with Oracle Mobile Security Suite.	For more information, see Section 10.13, "Getting Started with Oracle Mobile Security Suite After Installation."

10.4 Configuring Oracle Access Management in a WebLogic Domain

Oracle Access Management is required to run and use Oracle Mobile Security Suite. Before you begin configuring Oracle Mobile Security Suite, you must install and configure Oracle Access Management in a WebLogic domain. When you install and configure Oracle Access Management in a WebLogic domain, the Oracle Mobile Security Manager server is installed and configured in the domain by default. To

configure Oracle Access Management, follow the instructions in Chapter 5, "Configuring Oracle Access Management."

10.5 About the Administrator Roles in an Oracle Mobile Security Suite Deployment

An Oracle Mobile Security Suite deployment provides different administrator roles for the WebLogic Server, Oracle Access Manager, and Oracle Mobile Security Suite components. Before you begin configuring Oracle Mobile Security Suite, it is important to understand these roles and how to configure them.

For an Oracle Mobile Security Suite deployment, consider the following types of administrator roles:

- WebLogic Administrator Role, which provides administration privileges to configure WebLogic Server and provides authorization to access MBeans. Specifically, Mobile Security Access Server administration tasks are performed using MBeans, and therefore, this role is required.
- Oracle Access Manager Administrator Role, which provides administration privileges for the Oracle Access Manager component. This role provides authorization to perform Oracle Access Management configuration tasks on the Oracle Access Management Console.
- Oracle Mobile Security Suite Administrator Role, which provides administration privileges for Oracle Mobile Security Suite tasks, such as managing mobile devices and policies. All Oracle Mobile Security Suite tasks are performed on the Policy Manager Console running on the Policy Manager server. After Oracle Mobile Security Suite is fully configured with Oracle Access Manager, an Oracle Access Manager administrator is also configured as an Oracle Mobile Security Suite administrator.

To configure these roles for an Oracle Mobile Security Suite deployment, you need to do the following:

- Configure a common identity store, which is typically an enterprise directory.
- Create an administrator user and group in the directory, and then assign the user to the administrator group.
- Configure WebLogic Server, Oracle Access Manager, and Oracle Mobile Security Suite to use the same administrator group.

These configuration steps are described in the following tasks. These tasks must be completed to configure the required Oracle Mobile Security Suite administrator users, groups, and roles successfully.

- Preparing Your LDAP Directory as the Identity Store
- Configuring Oracle Access Manager for Oracle Mobile Security Suite
- Configuring Oracle Mobile Security Manager

As a result, once the administrator roles, users, and groups have been configured following these procedures, you will have a single admin user with full administration privileges over WebLogic Server, Oracle Access Manager, and Oracle Mobile Security Suite.

10.6 Preparing Your LDAP Directory as the Identity Store

Oracle Mobile Security Suite, along with other Oracle Identity and Access Management 11*g* Release 2 (11.1.2.3.0) components, relies on a specific set of user and groups to be present and correctly configured in the LDAP directory. As a result, you must prepare your LDAP directory to be able to configure a common identity store and a common administrator user and group for Oracle WebLogic Server, Oracle Access Manager, and Oracle Mobile Security Suite.

For information about preparing your LDAP directory, refer to one of the following procedures, depending on the type of LDAP directory you are using:

- To prepare Oracle Internet Directory (OID), Oracle Unified Directory (OUD), or Oracle Directory Server Enterprise Edition (ODSEE), perform the following tasks in the *Integration Guide for Oracle Identity Management Suite*:
  - "Extending Directory Schema for Access Manager"
  - "Creating Users and Groups for Access Manager"
  - "Creating Users and Groups for Oracle WebLogic Server"
- To prepare Microsoft Active Directory, perform the tasks described in "Preparing an Existing Microsoft Active Directory Instance for Use with Oracle Identity and Access Management" in the *Deployment Guide for Oracle Identity and Access Management*.

> **Note:** Before preparing your LDAP directory, ensure that the WebLogic Administration Server and LDAP server are running. For more information, see Appendix C.1, "Starting the Stack."

10.7 Configuring Oracle Access Manager for Oracle Mobile Security Suite

After you have prepared your LDAP directory, use the `idmConfigTool` command with the `-configOAM` option to configure your Oracle Access Manager Server that will be used with Oracle Mobile Security Suite. The command for running `idmConfigTool` is located in the *`IAM_HOME`*`/idmtools/bin` directory.

> **Note:** You should not execute the `idmConfigTool` command with the `-configOAM` option if your 11*g* Release 2 (11.1.2.3.0) environment was upgraded from an 11*g* Release 2 (11.1.2.2.0) environment where Oracle Access Manager was previously configured to use an external LDAP directory. In this case, you can skip section 10.7, but you must configure Oracle Mobile Security Manager, as described in Section 10.8, using exactly the same user, group, and LDAP directory properties that the upgraded Oracle Access Manager is already configured with.

Complete the following tasks to configure Oracle Access Manager:

- Creating the Oracle Access Manager Properties File
- Running idmConfigTool to Configure Oracle Access Manager
- Granting WebLogic Admin Role to Oracle Access Manager and WebLogic Server Groups
- Additional Task for Oracle Unified Directory

10.7.1 Creating the Oracle Access Manager Properties File

Use the guidelines below to create a properties file that will configure your Oracle Access Manager Server. You will pass this file to the `idmConfigTool` command in Section 10.7.2, "Running idmConfigTool to Configure Oracle Access Manager."

Create a file named `oam.properties` in the directory of your choice containing the properties described in Table 10–2.

> **Note:** For an example properties file that includes sample values, see Sample Oracle Access Manager Properties File.

Table 10–2 Oracle Access Manager Configuration Properties

Property	Description
Properties for connecting to Oracle WebLogic Server	
`WLSHOST`	The host name of your Oracle WebLogic Administration Server.
`WLSPORT`	The port number of your Oracle WebLogic Administration Server.
`WLSADMIN`	The Oracle WebLogic Server administrator user you use to log in to the WebLogic Administration Console.
Properties for configuring and connecting to the LDAP directory	
`IDSTORE_HOST`	The host name of your LDAP directory.
`IDSTORE_PORT`	The port number of your LDAP directory. This value can be a SSL port or a non-SSL port.
`IDSTORE_DIRECTORYTYPE`	Directory type of the LDAP server. Specify one of the following values. ■ `OID` if you are using Oracle Internet Directory. ■ `OUD` if you are using Oracle Unified Directory. ■ `IPLANET` if you are using ODSEE/iPlanet. ■ `AD` if you are using Microsoft Active Directory.
`IDSTORE_BINDDN`	An administrative user of the LDAP directory.
`IDSTORE_USERSEARCHBASE`	The location in the directory where users are stored. This property tells the directory where to search for users.
`IDSTORE_SEARCHBASE`	The location in the directory where users and groups are stored.
`IDSTORE_GROUPSEARCHBASE`	The location in the directory where groups (or roles) are stored. This property tells the directory where to search for groups or roles.
`IDSTORE_SYSTEMIDBASE`	The location of a container in the directory where system operations users should be stored so that they are kept separate from enterprise users stored in the main user container. The location of a container in the directory where `IDSTORE_OAMSOFTWAREUSER` is stored.
`OAM11G_IDSTORE_ROLE_SECURITY_ADMIN`	The name of the group that is used to allow access to the Oracle Access Management administration console.
`OAM11G_SERVER_LOGIN_ATTRIBUTE`	At a login attempt, the user name is validated against this attribute in the identity store.

Table 10–2 (Cont.) Oracle Access Manager Configuration Properties

Property	Description
OAM11G_IDSTORE_NAME	The identity store name. If you already have an identity store in place that you wish to reuse (rather than allowing the tool to create a new one for you), set this parameter to the name of the identity store you want to reuse.
OAM11G_CREATE_IDSTORE	Valid values are `true` or `false`.
IDSTORE_ USERNAMEATTRIBUTE	LDAP user name attribute used to search for users in the identity store.
IDSTORE_LOGINATTRIBUTE	An attribute of a user in the identity store that contains the user's login name. This is the attribute the user uses for login. This should be set to the same value as `OAM11G_SERVER_LOGIN_ ATTRIBUTE`.
IDSTORE_OAMSOFTWAREUSER	The user name used to establish the Oracle Access Manager identity store connection. Specify the name of the user that you created in Section 10.6, "Preparing Your LDAP Directory as the Identity Store." This user will be used by Oracle Access Manager to connect to the directory or LDAP server.
IDSTORE_OAMADMINUSER	The identity store administrator for Oracle Access Manager. Specify the name of a user that has privileges to access the Oracle Access Management Console. Specify the name of the user that you created in Section 10.6, "Preparing Your LDAP Directory as the Identity Store."
Properties for configuring WebGate	
WEBGATE_TYPE	The type of WebGate agent you want to create. Set to: ■ `ohsWebGate10g` if using WebGate version 10 ■ `ohsWebGate11g` if using WebGate version 11
ACCESS_GATE_ID	The name you want to assign to the WebGate.
COOKIE_DOMAIN	The web domain in which the WebGate functions. Specify the domain in the format `.cc.example.com`.
OAM11G_WG_DENY_ON_NOT_ PROTECTED	When set to `false`, this property allows login pages to be displayed. It should be set to `true` when using WebGate 11*g*. Valid values are `true` or `false`.
OAM_TRANSFER_MODE	The transfer mode for the Oracle Access Manager agent being configured. Valid values are `OPEN`, `SIMPLE`, or `CERT`.
Properties for configuring Oracle Access Manager Server	

Table 10–2 (Cont.) Oracle Access Manager Configuration Properties

Property	Description
OAM11G_SSO_ONLY_FLAG	This property configures Access Manager as authentication only mode or normal mode, which supports authentication and authorization. Specifies whether Oracle Access Manager server can perform authorizations. If `true`, the Oracle Access Manager 11*g* server operates in authentication only mode, where all authorizations return true by default without any policy validations. In this mode, the server does not have the overhead of authorization handling. This is recommended for applications that do not depend on authorization policies and need only the authentication feature of the Oracle Access Manager server. If `false`, the server runs in default mode, where each authentication is followed by one or more authorization requests to the Oracle Access Manager server. WebGate allows the access to the requested resources or not, based on the responses from the Oracle Access Manager server. Valid values are `true` (no authorization) or `false`.
OAM11G_OAM_SERVER_TRANSFER_MODE	The security model in which the Oracle Access Manager 11*g* server functions. Valid values are `OPEN` or `SIMPLE`.
PRIMARY_OAM_SERVERS	A comma-separated list of your Oracle Access Manager servers and their proxy ports. For example, `IDMHOST1:`*`OAM_PROXY_PORT`*.
OAM11G_IMPERSONATION_FLAG	Set to `true` to enable the OAM Impersonation feature. If this property is not set, the default value is `false`.
OAM11G_IDM_DOMAIN_LOGOUT_URLS	Comma-separated list of Oracle Access Manager logout URLs.
COOKIE_EXPIRY_INTERVAL	Cookie expiration period.
OAM11G_IDM_DOMAIN_OHS_HOST	Host name of the load balancer that is in front of Oracle HTTP Server.
OAM11G_IDM_DOMAIN_OHS_PORT	Port number on which the load balancer listens.
OAM11G_IDM_DOMAIN_OHS_PROTOCOL	Protocol for Oracle HTTP Server. Valid values are `http` or `https`.
OAM11G_SERVER_LBR_HOST	Host name of the load balancer front-ending the Oracle Access Manager server. This and the following two parameters are used to construct your login URL.
OAM11G_SERVER_LBR_PORT	The port number that the load balancer front-ending the Oracle Access Manager server is listening on.
OAM11G_SERVER_LBR_PROTOCOL	Protocol of the load balancer front-ending the Oracle Access Manager server. Valid values are `http` or `https`.
SPLIT_DOMAIN	Set to `true` if you are creating a domain with just Oracle Access Manager or Oracle Access Manager located in a separate domain from Oracle Identity Manager (split domain). Otherwise, it is not necessary to specify this parameter. Valid values are `true` or `false`. Set to `true` for cross-domain deployment.

Table 10–2 (Cont.) Oracle Access Manager Configuration Properties

Property	Description
Properties needed if you are configuring Oracle Identity Manager with Oracle Access Manager	
OAM11G_OIM_OHS_URL	The Oracle HTTP Server URL that front-ends the Oracle Identity Manager server. This property is only required if your topology contains Oracle Access Manager and Oracle Identity Manager.
OAM11G_OIM_INTEGRATION_REQ	This property specifies whether to integrate with Oracle Identity Manager or configure Oracle Access Manager in standalone mode. Set to `true` for integration. Valid values are `true` (integration) or `false`.

Sample Oracle Access Manager Properties File

```
WLSHOST: examplehost.example.com
WLSPORT: 7001
WLSADMIN: weblogic
IDSTORE_HOST: idstore.example.com
IDSTORE_PORT: 1389
IDSTORE_DIRECTORYTYPE: OUD
IDSTORE_BINDDN: cn=orcladmin
IDSTORE_USERSEARCHBASE: cn=Users,dc=example,dc=com
IDSTORE_SEARCHBASE: dc=example,dc=com
IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=example,dc=com
IDSTORE_SYSTEMIDBASE: cn=systemids,dc=example,dc=com
OAM11G_IDSTORE_ROLE_SECURITY_ADMIN: OAMAdministrators
OAM11G_SERVER_LOGIN_ATTRIBUTE: cn
OAM11G_CREATE_IDSTORE: true
OAM11G_IDSTORE_NAME: OAMIDSTORE
IDSTORE_USERNAMEATTRIBUTE: cn
IDSTORE_LOGINATTRIBUTE: cn
IDSTORE_OAMSOFTWAREUSER: oamLDAP
IDSTORE_OAMADMINUSER: oamadmin
WEBGATE_TYPE: ohsWebgate11g
ACCESS_GATE_ID: Webgate_IDM
COOKIE_DOMAIN: .cc.example.com
OAM11G_WG_DENY_ON_NOT_PROTECTED: true
OAM_TRANSFER_MODE: open
OAM11G_SSO_ONLY_FLAG: false
OAM11G_OAM_SERVER_TRANSFER_MODE: open
PRIMARY_OAM_SERVERS: examplehost.example.com:5575
OAM11G_IMPERSONATION_FLAG: false
OAM11G_IDM_DOMAIN_LOGOUT_URLS: /oamsso/logout.html,
/console/jsp/common/logout.jsp, /em/targetauth/emaslogout.jsp
COOKIE_EXPIRY_INTERVAL: 120
OAM11G_IDM_DOMAIN_OHS_HOST: examplehost.example.com
OAM11G_IDM_DOMAIN_OHS_PORT: 7777
OAM11G_IDM_DOMAIN_OHS_PROTOCOL: http
OAM11G_SERVER_LBR_HOST: examplehost.example.com
OAM11G_SERVER_LBR_PORT: 7777
OAM11G_SERVER_LBR_PROTOCOL: http
SPLIT_DOMAIN: true
OAM11G_OIM_OHS_URL: http://examplehost.example.com:7778
OAM11G_OIM_INTEGRATION_REQ: false
```

10.7.2 Running idmConfigTool to Configure Oracle Access Manager

To configure Oracle Access Manager, run the `idmConfigTool` command with the `-configOAM` option as follows:

Note:

Before running `idmConfigTool`:

- Make sure that you have created the required properties file, as described in Section 10.7.1, "Creating the Oracle Access Manager Properties File."
- Ensure that the WebLogic Administration Server and LDAP server are running. For more information, see Appendix C.1, "Starting the Stack."

---

1. Set the following environment variables:
   - Set `MW_HOME` to the full path of the Oracle Identity and Access Management Middleware home. Enter the path to the Middleware home that was created when you installed Oracle WebLogic Server 11*g* Release 1 (10.3.6) on your system. For example, `/u01/oracle/products/fmw_oam`.
   - Set `ORACLE_HOME` to the full path of the Oracle home where Oracle Access Manager is installed. Set to the location of your *`IAM_HOME`* directory. For example, `/u01/oracle/products/fmw_oam/Oracle_IDM1`.
   - Set `JAVA_HOME` to the full path of the JDK directory.
2. Change directory to the *`IAM_HOME`*`/idmtools/bin` directory:

   ```
   cd IAM_HOME/idmtools/bin
   ```

3. Run the following command:

   ```
   idmConfigTool.sh -configOAM input_file=configfile log_level=level log_file=log_file
   ```

   Where
   - (Required) `input_file` is the full or relative path to the properties file you created in Section 10.7.1, "Creating the Oracle Access Manager Properties File."
   - (Optional) `log_level` is the level of logging performed by `idmConfigTool`. Possible values are `ALL`, `SEVERE`, `WARNING`, `INFO`, `CONFIG`, `FINE`, `FINER`, and `FINEST`. If not specified, the default is `INFO`.
   - (Optional) `log_file` is the full or relative path to the file where `idmConfigTool` will store the log file data. If not specified, `idmConfigTool` creates a log file named `automation.log` in the directory where you run the tool.

   For example:

   ```
   idmConfigTool.sh -configOAM input_file=oam.properties
   ```

   Where `oam.properties` is a properties file containing configuration parameters specific to your environment. For information on creating this file, see Section 10.7.1, "Creating the Oracle Access Manager Properties File."

When the command runs, it prompts you to enter the password of the account used to connect to the identity store. It also prompts you to enter passwords for the following:

- `OAM11G_WLS_ADMIN_PASSWD`: Enter the password for the WebLogic Server Administrator user (`WLSADMIN`).
- `OAM11G_IDM_DOMAIN_WEBGATE_PASSWD`: Enter a password to be assigned to the WebGate.
- `IDSTORE_PWD_OAMSOFTWAREUSER`: Enter the password for `IDSTORE_OAMSOFTWAREUSER`.
- `IDSTORE_PWD_OAMADMINUSER`: Enter the password for `IDSTORE_OAMADMINUSER`.

Sample command output, when running the command against Oracle Unified Directory:

```
Enter ID Store Bind DN password:
Enter User Password for OAM11G_WLS_ADMIN_PASSWD:
Confirm User Password for OAM11G_WLS_ADMIN_PASSWD:
Enter User Password for OAM11G_IDM_DOMAIN_WEBGATE_PASSWD:
Confirm User Password for OAM11G_IDM_DOMAIN_WEBGATE_PASSWD:
Enter User Password for IDSTORE_PWD_OAMSOFTWAREUSER:
Confirm User Password for IDSTORE_PWD_OAMSOFTWAREUSER:
Enter User Password for IDSTORE_PWD_OAMADMINUSER:
Confirm User Password for IDSTORE_PWD_OAMADMINUSER:
Connecting to t3://examplehost.example.com:7001
Connection to domain runtime mbean server established
Starting edit session
Edit session started
Connected to security realm.
Validating provider configuration
Validated desired authentication providers
Created OAMIDAsserter successfuly
Created OUDAuthenticator successfuly
Setting attributes for OUDAuthenticator
All attributes set. Configured inOUDAuthenticatornow
LDAP details configured in OUDAuthenticator
Dec 19, 2014 6:40:38 AM
oracle.idm.automation.impl.oam.handlers.WLSAuthnConfigHandler logInfo
INFO: ControlFlag for OAMIDAsserter set to REQUIRED
Dec 19, 2014 6:40:38 AM
oracle.idm.automation.impl.oam.handlers.WLSAuthnConfigHandler logInfo
INFO: ControlFlag for OUDAuthenticator set to SUFFICIENT
Dec 19, 2014 6:40:38 AM
oracle.idm.automation.impl.oam.handlers.WLSAuthnConfigHandler logInfo
INFO: ControlFlag for DefaultAuthenticator set to SUFFICIENT
Control flags for authenticators set sucessfully
Dec 19, 2014 6:40:38 AM
oracle.idm.automation.impl.oam.handlers.WLSAuthnConfigHandler logInfo
INFO: Total providers - 5
Reordering of authenticators done sucessfully
Saving the transaction
Transaction saved
Activating the changes
Changes Activated. Edit session ended.
Connection closed sucessfully
The tool has completed its operation. Details have been logged to
automation.log
```

Sample command output, when running the command against Microsoft Active Directory:

```
Enter ID Store Bind DN password:
Enter User Password for OAM11G_WLS_ADMIN_PASSWD:
Confirm User Password for OAM11G_WLS_ADMIN_PASSWD:
Enter User Password for OAM11G_IDM_DOMAIN_WEBGATE_PASSWD:
Confirm User Password for OAM11G_IDM_DOMAIN_WEBGATE_PASSWD:
Enter User Password for IDSTORE_PWD_OAMSOFTWAREUSER:
Confirm User Password for IDSTORE_PWD_OAMSOFTWAREUSER:
Enter User Password for IDSTORE_PWD_OAMADMINUSER:
Confirm User Password for IDSTORE_PWD_OAMADMINUSER:
Connecting to t3://examplehost.example.com:7001
Connection to domain runtime mbean server established
Starting edit session
Edit session started
Connected to security realm.
Validating provider configuration
Validated desired authentication providers
OAM Asserter already exists in the security realm
Created ADAuthenticator successfuly
Setting attributes for ADAuthenticator
All attributes set. Configured inADAuthenticatornow
LDAP details configured in ADAuthenticator
Control flags for authenticators set sucessfully
Reordering of authenticators done sucessfully
Saving the transaction
Transaction saved
Activating the changes
Changes Activated. Edit session ended.
Connection closed sucessfully
The tool has completed its operation. Details have been logged to oam.log
```

4. Check the log file for any errors or warnings and correct them before continuing.
5. Restart the Oracle WebLogic Administration Server, as described in Appendix C.3, "Restarting Servers."

10.7.3 Granting WebLogic Admin Role to Oracle Access Manager and WebLogic Server Groups

After you complete the installation process, you do not have any users or groups present with the WebLogic administrator role. Perform the following steps to grant the WebLogic Admin role to the Oracle Access Manager administrator group and to the WebLogic Server administrator group.

1. Log in to the WebLogic Server Administration Console.
2. Click **Security Realms** from the **Domain Structure** menu.
3. Click **myrealm** in the Realms table.
4. Click the **Roles and Policies** tab.
5. Expand the **Global Roles** entry in the Roles table. This brings up the entry for Roles.
6. Click **Roles** under the **Global Roles** entry.
7. Click the **Admin** role in the Global Roles table.
8. Under **Role Conditions**, click **Add Conditions**.

9. Select **Group** from the predicate list and click **Next**.
10. In the **Group Argument Name** field, enter the name of the Oracle Access Manager administrator group (`OAM11G_IDSTORE_ROLE_SECURITY_ADMIN`) that you created in Section 10.6, "Preparing Your LDAP Directory as the Identity Store." For example, `OAMAdministrators`.

    Click **Add**.
11. Click **Finish**.

    Role Conditions now shows the Oracle Access Manager administrator group as an entry.
12. Under **Role Conditions**, click **Add Conditions**.
13. Select **Group** from the predicate list and click **Next**.
14. In the **Group Argument Name** field, enter the name of the WebLogic Server administrator group (`IDSTORE_WLSADMINGROUP`) that you created in Section 10.6, "Preparing Your LDAP Directory as the Identity Store." For example, `IDM Administrators`.

    Click **Add**.
15. Click **Finish**.

    Role Conditions now shows the WebLogic Server administrator group as an entry.
16. Click **Save** and then restart the Administration Server.

10.7.4 Additional Task for Oracle Unified Directory

If you are using Oracle Unified Directory (OUD) as the LDAP identity store and the group object class is `groupOfUniqueNames`, perform the following additional steps:

1. Connect to the WebLogic Administration Server using the WLST `connect` command:

```
IAM_HOME/common/bin/wlst.sh
connect()
```

2. Run the following WLST commands in this order:

> **Note:** Replace *domain_name* with the name of the domain that you created in Section 10.4, "Configuring Oracle Access Management in a WebLogic Domain."

```
edit()

startEdit()

cd('/SecurityConfiguration/domain_
name/Realms/myrealm/AuthenticationProviders/OUDAuthenticator')

cmo.setStaticMemberDNAttribute('uniquemember')

cmo.setStaticGroupDNsfromMemberDNFilter('(&(uniquemember=%M)(objectclass=groupO
fUniqueNames))')

cmo.setStaticGroupObjectClass('groupOfUniqueNames')
```

```
activate()
```

10.8 Configuring Oracle Mobile Security Manager

After you have executed the `idmConfigTool -configOAM` command to configure Oracle Access Manager, use `idmConfigTool` to configure the identity store, keystores, and trust stores for the Oracle Mobile Security Manager Server.

Complete the following tasks to configure Oracle Mobile Security Manager:

- Creating the Oracle Mobile Security Suite Properties File
- Running idmConfigTool to Configure Oracle Mobile Security Manager

10.8.1 Creating the Oracle Mobile Security Suite Properties File

Use the guidelines below to create a properties file that will configure your Oracle Mobile Security Manager Server. You will pass this file to the `idmConfigTool` command in Section 10.8.2, "Running idmConfigTool to Configure Oracle Mobile Security Manager."

Create a file named `omss.properties` in the directory of your choice containing the properties described in Table 10–3. Note that all properties are required unless marked as (Optional).

Notes:

- For an example properties file that includes sample values, see Sample Oracle Mobile Security Suite Properties File.
- Oracle Access Manager and Oracle Mobile Security Manager must point to the same identity store when you run `idmConfigTool -configOAM` and `idmConfigTool -configOMSS mode=OMSM` to configure Oracle Access Manager and Oracle Mobile Security Manager, respectively.
- Make sure to save this file. You will use this properties file later for Mobile Security Access Server configuration. To configure Mobile Security Access Server, you run the `idmConfigTool` command with the `-configOMSS mode=OMSAS` option. For more information, see "Configuring the Identity Store and Keystores for the MSAS Instance" in *Installing Oracle Mobile Security Access Server*.

Table 10–3 Oracle Mobile Security Suite Configuration Properties

Property	Description
Properties for configuring and connecting to the LDAP directory	
`IDSTORE_SSL_ENABLED`	(Optional) Set to `true` if you want to communicate with the LDAP directory using SSL. The default value is `false`.

Table 10–3 (Cont.) Oracle Mobile Security Suite Configuration Properties

Property	Description
IDSTORE_DIRECTORYTYPE	Directory type of the LDAP Server. Specify one of the following values. ■ OID if you are using Oracle Internet Directory. ■ OUD if you are using Oracle Unified Directory. ■ ODSEE if you are using ODSEE/iPlanet. ■ AD if you are using Microsoft Active Directory.
IDSTORE_HOST	The host name of your LDAP directory. This should be the same value that you used for this property when you created the Oracle Access Manager properties file in Section 10.7.1, "Creating the Oracle Access Manager Properties File."
IDSTORE_PORT	The port number of your LDAP directory. This value can be a SSL port or a non-SSL port. This should be the same value that you used for this property when you created the Oracle Access Manager properties file in Section 10.7.1, "Creating the Oracle Access Manager Properties File."
IDSTORE_SSL_CERT_PATH	(Optional) Specify the absolute path to the location that contains directory-specific SSL certificates. This property is applicable only if the LDAP directory communicates over a SSL port. If provided, idmConfigTool will load all the certificate files that are present in this location. These certificates should be in .cer format.
IDSTORE_BINDDN	An administrative user of the LDAP directory.
IDSTORE_ USERNAMEATTRIBUTE	LDAP user name attribute used to search for users in the identity store.
IDSTORE_USERSEARCHBASE	The location in the directory where users are stored. This property tells the directory where to search for users.
IDSTORE_GROUPSEARCHBASE	The location in the directory where groups (or roles) are stored. This property tells the directory where to search for groups or roles.
IDSTORE_SEARCHBASE	The location in the directory where users and groups are stored.
IDSTORE_LOGINATTRIBUTE	An attribute of a user in the identity store that contains the user's login name. This is the attribute the user uses for login.
OMSS_OMSM_IDSTORE_ PROFILENAME	Name of the identity store profile for Oracle Mobile Security Manager. The idmConfigTool command will create an identity store profile for Mobile Security Manager with this name. It is used by Mobile Security Manager to connect to the identity store.
Properties for connecting to Oracle WebLogic Server	
WLSHOST	The host name of your Oracle WebLogic Administration Server.
WLSADMIN	The WebLogic Server Administrator user you use to log in to the WebLogic Administration Console.
WLSPORT	The port number of your WebLogic Administration Server.
OMSS_DOMAIN_LOCATION	The absolute path to the Oracle Mobile Security Manager domain you created in Section 10.4, "Configuring Oracle Access Management in a WebLogic Domain."

Table 10–3 (Cont.) Oracle Mobile Security Suite Configuration Properties

Property	Description
Properties for configuring Oracle Mobile Security Suite users, groups, and roles	
OMSS_IDSTORE_ROLE_SECURITY_ADMIN	(Optional) Name of the administrator group whose members have administrative privileges for Oracle Mobile Security Manager operations. This group is used to allow access to the Oracle Mobile Security Manager features on the Policy Manager Console. This should be set to the same value that you provided for OAM11G_IDSTORE_ROLE_SECURITY_ADMIN in the Oracle Access Manager properties file. The default value is MSMSysAdminUsers.
OMSS_IDSTORE_ROLE_SECURITY_HELPDESK	(Optional) Name of the Oracle Mobile Security Manager helpdesk group, whose members get helpdesk privileges for Oracle Mobile Security Manager operations. This group is used to allow access to the Security Help Desk privileges in the Policy Manager Console. The default value is MSMHelpdeskUsers.
OMSS_SCEP_DYNAMIC_CHALLENGE_USER	(Optional) Oracle Mobile Security Manager uses a Simple Certificate Enrollment Protocol (SCEP) dynamic challenge for external SCEP authorization during the enrollment phase. Mobile Security Manager will use this user for authentication.
Properties for Mobile Security Manager Server and Policy Manager Server	
OMSS_OMSM_SERVER_NAME	Name of the Mobile Security Manager Managed Server. By default, this is omsm_server1. Provide this only if the Oracle Mobile Security Manager Server is renamed to a different value during domain configuration. This property must match the Mobile Security Manager Server name(s) provided during domain configuration. If you have multiple Mobile Security Manager Servers, specify a comma-separated list of Managed Server names. For example, WLS_MSM1, WLS_MSM2.
OMSS_OMSM_SERVER_HOST	(Optional) A comma-separated list of the hosts on which your Mobile Security Manager Servers are assigned. The number and order of the hosts specified for OMSS_OMSM_SERVER_HOST must match the number and order of servers specified for OMSS_OMSM_SERVER_NAME. If this property is not specified in the properties file, idmConfigTool queries the WebLogic domain configuration to obtain the host information.
OMSS_OAM_POLICY_MGR_SERVER_NAME	Name of the Policy Manager Managed Server. By default, this is oam_policy_mgr1. Provide this only if the Policy Manager Server is renamed to a different value during domain configuration. This property must match the Policy Manager Server name(s) provided during domain configuration.
Properties for a cluster deployment	

Table 10–3 (Cont.) Oracle Mobile Security Suite Configuration Properties

Property	Description
OMSS_OMSM_FRONT_END_URL	(Optional) For cluster deployments, provide the URL of the load balancer that front-ends the Oracle Mobile Security Manager cluster. This property is not required if Mobile Security Manager is not deployed in a cluster. It is required only if there is a cluster of Mobile Security Manager servers. The OMSS_OMSM_FRONT_END_URL is of the format http://*host*:*port* or https://*host*:*sslport*
Properties for configuring and connecting to a proxy server	
OMSS_PROXY_SERVER_HOST	(Optional) If you are using a proxy server, specify the host name of the proxy server. This and the following three properties are required if the Mobile Security Manager Server will be running within an internal network and will require a proxy server to communicate to an outside network.
OMSS_PROXY_SERVER_PORT	(Optional) If you are using a proxy server, specify the port number of the proxy server.
OMSS_PROXY_USER	(Optional) The user name for connecting to the proxy server. If the proxy server is unauthenticated, then OMSS_PROXY_USER is not required.
OMSS_USE_PROXY	(Optional) Valid values are true or false. If true, proxy server will be enabled. If false, proxy server will be disabled.
Properties for connecting to the database	
OMSS_JDBC_URL	Specify the JDBC URL to the Oracle Mobile Security Manager database repository, in the following format, where *db_host* is the host name of the machine on which the database resides, *port* is the listener port of the database, and *service_name* is the service name identified for the database. This URL will be used to seed Apple Push Notification Service (APNs)/Google Cloud Messaging (GCM) data. jdbc:oracle:thin:@*db_host*:*port*/*service_name* For example jdbc:oracle:thin:@examplehost.exampledomain.com:1521/orcl.example.com
OMSS_OMSM_SCHEMA_USER	The user name for the Oracle Mobile Security Manager schema, which consists of the prefix that was configured for the repository in RCU followed by _OMSM.
Properties for configuring GCM and APNs	

Table 10–3 (Cont.) Oracle Mobile Security Suite Configuration Properties

Property	Description
OMSS_GCM_SENDER_ID	(Optional) Google Cloud Messaging (GCM) notification sender ID. This property is required for Android Mobile Device Management (MDM) functionality. Mobile Security Manager requires GCM credentials to connect to GCM and send push notifications to Android devices. If you are planning to use MDM, you can choose to configure GCM during configuration using idmConfigTool or configure GCM manually after configuration using the Policy Manager Console. Set this property to the project number of the Google API Project you created. For more information, including how to create a Google API Project and obtain a GCM API key, see "Configuring the GCM Entry" in *Administering Oracle Mobile Security Suite*.
OMSS_APNS_FILE	(Optional) The full path and file name of the Apple Push Notification Service (APNs) keystore file, which is used to establish secure connection to Apple server and to send notifications. The APNs keystore file is required for iOS Mobile Device Management (MDM) functionality. Mobile Security Manager requires an Apple MDM certificate to manage iOS devices. This certificate enables secure communication using Apple Push Notification Services (APNs). If you are planning to use MDM, you can choose to configure APNs during configuration using idmConfigTool or configure APNs manually after configuration using the Policy Manager Console. For more information, including how to obtain a APNs certificate file, see "Configuring the APNS Certificate" in *Administering Oracle Mobile Security Suite*.
Properties for configuring Exchange server and email settings	
OMSS_EXCHANGE_DOMAIN_NAME	(Optional) Specify the domain name of the Exchange server that Oracle Mobile Security Suite will connect to. If specified, you must also enter values for the following four OMSS_EXCHANGE properties in this file.
OMSS_EXCHANGE_SERVER_URL	(Optional) Specify the URL of the Exchange server that Oracle Mobile Security Suite will connect to. If specified, you must also enter values for all the other OMSS_EXCHANGE properties.
OMSS_EXCHANGE_LISTENER_URL	(Optional) Specify the listener URL of the Exchange server that Oracle Mobile Security Suite will connect to. If specified, you must also enter values for all the other OMSS_EXCHANGE properties.
OMSS_EXCHANGE_SERVER_VERSION	(Optional) Specify the version number of the Exchange server that Oracle Mobile Security Suite will connect to. If specified, you must also enter values for all the other OMSS_EXCHANGE properties.
OMSS_EXCHANGE_ADMIN_USER	(Optional) Specify the administrative user name of the Exchange server that Oracle Mobile Security Suite will connect to. If specified, you must also enter values for all the other OMSS_EXCHANGE properties.

Table 10–3 (Cont.) Oracle Mobile Security Suite Configuration Properties

Property	Description
OMSS_EMAIL_ADMIN_USER	(Optional) Specify the Oracle Mobile Security Suite email administrator user name, which must be an email address. If specified, you must also enter values for the following two properties, which are used by Mobile Security Manager to send email invites to users.
OMSS_SMTP_HOST	(Optional) Specify the host name of the SMTP server that Oracle Mobile Security Manager will use to send email invites to users. If specified, you must also enter values for OMSS_EMAIL_ADMIN_USER and OMSS_SMTP_PORT.
OMSS_SMTP_PORT	(Optional) Specify the port number of the SMTP server that Oracle Mobile Security Manager will use to send email invites to users. If specified, you must also enter values for OMSS_EMAIL_ADMIN_USER and OMSS_SMTP_HOST.
OMSS_OMSM_SERVER_KEY_LENGTH	(Optional) The key length (in bits) for the self-signed CA and generated keys for the Oracle Mobile Security Manager server. The default value is 2048.
Properties for Mobile Security Access Server	
OMSS_MSAS_SERVER_HOST	The host name for Oracle Mobile Security Access Server. If the Mobile Security Access Server instance is behind a load balancer, provide the host name of the load balancer. Note that this and the OMSS_MSAS_SERVER_PORT property are required to run the idmConfigTool -configOMSS mode=OMSM command, as described in Section 10.8.2, and the idmConfigTool -configOMSS mode=OMSAS command, as described in *Installing Oracle Mobile Security Access Server*.
OMSS_MSAS_SERVER_PORT	The SSL port where the Oracle Mobile Security Access Server instance will be running If the Mobile Security Access Server instance is behind a load balancer, provide the port number of the load balancer.
Properties required only for configuring Mobile Security Access Server using the idmConfigTool -configOMSS mode=OMSAS command	
OMSS_OMSAS_AUX_CERTIFICATES_LOCATION	(Optional) This value should be a directory location. This location contains certificates that are used for establishing authentication and trust whenever the Mobile Security Manager Server interacts with external directories or authentication servers. All certificate files present within this location will be added to the Mobile Security Access Server trust stores. This and the following two properties are required for Mobile Security Access Server configuration. Note that these properties are required only to run the idmConfigTool -configOMSS mode=OMSAS command. For more information, see "Configuring the Identity Store and Keystores for the MSAS Instance" in *Installing Oracle Mobile Security Access Server*.

Table 10–3 (Cont.) Oracle Mobile Security Suite Configuration Properties

Property	Description
OMSS_OMSAS_IDSTORE_PROFILENAME	Name of the identity store profile for Oracle Mobile Security Access Server. The `idmConfigTool` command will create an identity store profile for Mobile Security Access Server with this name.
OMSS_GATEWAY_INSTANCE_ID	The name of the Oracle Mobile Security Access Server gateway instance. You can create and configure the Mobile Security Access Server gateway instance only after you have installed Mobile Security Access Server. For more information, see *Installing Oracle Mobile Security Access Server*.

Sample Oracle Mobile Security Suite Properties File

```
IDSTORE_SSL_ENABLED: false
IDSTORE_DIRECTORYTYPE: OUD
IDSTORE_HOST: idstore.example.com
IDSTORE_PORT: 1389
#IDSTORE_SSL_CERT_PATH: path_to_directory_containing_ssl_certificates
IDSTORE_BINDDN: cn=orcladmin
IDSTORE_USERNAMEATTRIBUTE: cn
IDSTORE_USERSEARCHBASE: cn=Users,dc=example,dc=com
IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=example,dc=com
IDSTORE_SEARCHBASE: dc=example,dc=com
IDSTORE_LOGINATTRIBUTE: cn
OMSS_OMSM_IDSTORE_PROFILENAME: msmprofile
WLSHOST: examplehost.example.com
WLSADMIN: weblogic
WLSPORT: 7001
OMSS_DOMAIN_LOCATION: /u01/oracle/admin/oam/user_projects/domains/oam_domain
OMSS_IDSTORE_ROLE_SECURITY_ADMIN: OAMAdministrators
OMSS_IDSTORE_ROLE_SECURITY_HELPDESK: MSMHelpdeskUsers
OMSS_SCEP_DYNAMIC_CHALLENGE_USER: adminuser
OMSS_OMSM_SERVER_NAME: WLS_MSM1
OMSS_OMSM_SERVER_HOST: examplehost1.example.com
OMSS_OAM_POLICY_MGR_SERVER_NAME: WLS_AMA1
OMSS_OMSM_FRONT_END_URL: http://lbr-machine:7777
OMSS_PROXY_SERVER_HOST: www-proxy.example.com
OMSS_PROXY_SERVER_PORT: 80
OMSS_PROXY_USER: proxyuser
OMSS_USE_PROXY: false
OMSS_JDBC_URL: jdbc:oracle:thin:@examplehost.example.com:1521/msmdb.example.com
OMSS_OMSM_SCHEMA_USER: DEV3_OMSM
OMSS_GCM_SENDER_ID: 610046050155
OMSS_APNS_FILE: /scratch/keystores/APNS.p12
OMSS_EXCHANGE_DOMAIN_NAME: test.com
OMSS_EXCHANGE_SERVER_URL: http://testuri.com
OMSS_EXCHANGE_LISTENER_URL: http://testuri.com
OMSS_EXCHANGE_SERVER_VERSION: 2.0
OMSS_EXCHANGE_ADMIN_USER: serviceuser
OMSS_EMAIL_ADMIN_USER: admin@acme.com
OMSS_SMTP_HOST: exchangeurl.example.com
OMSS_SMTP_PORT: 80
OMSS_OMSM_SERVER_KEY_LENGTH: 2048
OMSS_MSAS_SERVER_HOST: examplehost.example.com
OMSS_MSAS_SERVER_PORT: 9001
OMSS_OMSAS_AUX_CERTIFICATES_LOCATION:
OMSS_OMSAS_IDSTORE_PROFILENAME: msasprofile
```

```
OMSS_GATEWAY_INSTANCE_ID: msas_gateway-1
```

10.8.2 Running idmConfigTool to Configure Oracle Mobile Security Manager

Perform the steps in this section to run the `idmConfigTool -configOMSS mode=OMSM` command. This command configures the identity store, keystores, and trust stores for Oracle Mobile Security Manager.

Note:

Before running `idmConfigTool`:

- Make sure that you have created the required properties file, as described in Section 10.8.1, "Creating the Oracle Mobile Security Suite Properties File."
- Ensure that the WebLogic Administration Server and LDAP server are running. At this point, Managed Servers should be down. For more information, see Appendix C.1, "Starting the Stack."
- Note that Oracle Access Manager and Oracle Mobile Security Manager must be configured against the same identity store when you run `idmConfigTool -configOAM` and `idmConfigTool -configOMSS mode=OMSM` to configure Oracle Access Manager and Oracle Mobile Security Manager, respectively.

---

1. Set the following environment variables:
   - Set `MW_HOME` to the full path of the Oracle Identity and Access Management Middleware home. 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. For example, `/u01/oracle/products/fmw_oam`.
   - Set `ORACLE_HOME` to the full path of the Oracle home where Oracle Access Manager and Oracle Mobile Security Manager are installed. Set to the location of your *`IAM_HOME`* directory. For example, `/u01/oracle/products/fmw_oam/Oracle_IDM1`.
   - Set `WL_HOME` to the top-level directory of your Oracle WebLogic Server installation. For example, `/u01/oracle/products/fmw_oam/wlserver_10.3`.
   - Set `JAVA_HOME` to the full path of the JDK directory.
2. Change directory to the *`IAM_HOME`*`/idmtools/bin` directory:

   ```
   cd IAM_HOME/idmtools/bin
   ```

3. Run the following command:

   ```
   idmConfigTool.sh -configOMSS mode=OMSM input_file=configfile log_level=level
   log_file=log_file
   ```

   Where
   - (Required) `input_file` is the full or relative path to the properties file you created in Section 10.8.1, "Creating the Oracle Mobile Security Suite Properties File."

- (Optional) `log_level` is the level of logging performed by `idmConfigTool`. Possible values are `ALL`, `SEVERE`, `WARNING`, `INFO`, `CONFIG`, `FINE`, `FINER`, and `FINEST`. If not specified, the default is `INFO`.
- (Optional) `log_file` is the full or relative path to the file where `idmConfigTool` will store the log file data. If not specified, `idmConfigTool` creates a log file named `automation.log` in the directory where you run the tool.

For example:

```
idmConfigTool.sh -configOMSS mode=OMSM input_file=omss.properties
```

Where `omss.properties` is a properties file containing configuration parameters specific to your environment. For information on creating this file, see Section 10.8.1, "Creating the Oracle Mobile Security Suite Properties File."

Note: This command creates the following files in the *DOMAIN_HOME*`/config/fmwconfig` directory for the Oracle Mobile Security Manager Server:

- `server-identity.jks`: This keystore is used to validate the identity of the Oracle Mobile Security Manager Server when accessed by a Mobile Security Access Server instance.
- `wlstrust.jks`: This trust store stores trusted certificates so that Oracle Mobile Security Manager can trust other entities, such as your Mobile Security Access Server instance, database, and Directory Server. However, an administrator might still need to import additional trusted certificates into `wlstrust.jks` whenever required.

When the command runs, it prompts you to enter the password of the account used to connect to the identity store. It also prompts you to enter passwords for the following:

- `Enter OMSS Keystore Password:` Enter a password that will be used to generate Mobile Security Manager keystores and keys.
- `Enter Email User Password:` This prompt is displayed only if you entered a value for `OMSS_EMAIL_ADMIN_USER` in the properties file. Enter the password for the Oracle Mobile Security Suite email administrator (`OMSS_EMAIL_ADMIN_USER`).
- `Enter Exchange User Password:` This prompt is displayed only if you entered a value for `OMSS_EXCHANGE_ADMIN_USER` in the properties file. Enter the password for the Exchange server's administrative user (`OMSS_EXCHANGE_ADMIN_USER`).
- `Enter Proxy User Password:` This prompt is displayed only if you entered a value for `OMSS_PROXY_USER` in the properties file. Enter the password for connecting to the proxy server.
- `Enter SCEP Dynamic Challenge Password:` This prompt is displayed only if you entered a value for `OMSS_SCEP_DYNAMIC_CHALLENGE_USER` in the properties file. Enter the password for the SCEP Dynamic Challenge user (`OMSS_SCEP_DYNAMIC_CHALLENGE_USER`).
- `Enter OMSM Schema User Password:` Enter the password for the Oracle Mobile Security Manager schema.

- `Enter APNS Keystore Password`: This prompt is displayed only if you entered a value for `OMSS_APNS_FILE` in the properties file. Enter the Apple Push Notification Service (APNs) keystore password.
- `Enter GCM API Key`: This prompt is displayed only if you entered a value for `OMSS_GCM_SENDER_ID` in the properties file. Enter the API key value for Google Cloud Messaging (GCM) notifications.
- `Enter Weblogic Password`: Enter the password for the WebLogic Server Administrator user (`WLSADMIN`).

Sample command output:

```
Enter ID Store Bind DN Password:
Enter OMSS Keystore Password:
Enter Email User Password:
Enter Exchange User Password:
Enter Proxy User Password:
Enter SCEP Dynamic Challenge Password:
Enter OMSM Schema User Password:
Enter APNS Keystore Password:
Enter GCM API Key:
Enter Weblogic Password:
(1/8) MSM Configurations                          Success
(2/8) Seeding User Notification Templates         Success
(3/8) Seeding CSF Credentials                     Success
(4/8) Configuring IDS Profile                     Success
(5/8) Configuring OMSS Authentication Provider    Success
(6/8) Creating MSM Keystores                      Success
(7/8) Configuring MSM Server's SSL                Success
(8/8) OAM Console Integration                     Success
```

4. Check the log file for any errors or warnings and correct them before continuing.
5. Restart the WebLogic Administration Server for certain changes to take effect.

Note: After you have completed all the required configuration steps, as described in the Configuration Roadmap for Oracle Mobile Security Suite, the default administrator roles, users, and groups for your Oracle Mobile Security Suite deployment are configured as follows:

- The Oracle Access Manager administrator user (`IDSTORE_OAMADMINUSER`) is a member of the Oracle Access Manager administrator group (`OAM11G_IDSTORE_ROLE_SECURITY_ADMIN`) in the identity store.
- The Oracle Access Manager administrator group (`OAM11G_IDSTORE_ROLE_SECURITY_ADMIN`) is a member of the WebLogic Server administrator group (`IDSTORE_WLSADMINGROUP`) in the identity store.
- The WebLogic Server administrator user (`IDSTORE_WLSADMINUSER`) is a member of the WebLogic Server administrator group (`IDSTORE_WLSADMINGROUP`) in the identity store.
- The WebLogic Server administrator group (`IDSTORE_WLSADMINGROUP`) maps to the WebLogic Admin role in WebLogic Server.
- The Oracle Access Manager administrator group (`OAM11G_IDSTORE_ROLE_SECURITY_ADMIN`) maps to the Oracle Access Manager admin role in Oracle Access Manager.

These five statements together give you two users: `IDSTORE_OAMADMINUSER` and `IDSTORE_WLSADMINUSER`. These two users are granted the following privileges:

- The `IDSTORE_OAMADMINUSER` user has full administration privileges over Oracle WebLogic Server, Oracle Access Manager, and Oracle Mobile Security Suite components. This user can log in to the WebLogic Server Administration Console, the Oracle Access Management Console, and the Policy Manager Console (to access the Mobile Security Manager pages) without any authentication or authorization issues.
- The `IDSTORE_WLSADMINUSER` user has full administration privileges over WebLogic Server only. This user is granted administrator privileges on the WebLogic Server Administration Console. Note that this user can only be used for WebLogic Server administration. This user cannot be used for Oracle Access Management and Oracle Mobile Security Suite administration.

If you want to create and add additional administrator groups after configuration, see Section 10.11, "Optional: Creating Additional Administrator Groups After Configuration."

Note: After running the `idmConfigTool -configOMSS mode=OMSM` command, you can create Managed Servers on remote machines by using the `pack` and `unpack` commands. For more information, see "Creating and Starting a Managed Server on a Remote Machine" in *Creating Templates and Domains Using the Pack and Unpack Commands*.

10.9 Starting the Managed Servers

After successfully running the `idmConfigTool -configOMSS mode=OMSM` command, start the Managed Servers for Oracle Access Manager (`WLS_OAM1`), Access Manager Policy Manager (`WLS_AMA1`), and Oracle Mobile Security Manager (`WLS_MSM1`). For more information, see Appendix C.1, "Starting the Stack."

10.10 Verifying Oracle Access Manager and Oracle Mobile Security Manager

Verify the configuration of Oracle Mobile Security Manager and Oracle Access Manager, as follows:

1. Ensure that the following servers are up and running:
   - Oracle WebLogic Administration Server
   - Oracle Access Manager Managed Server (`WLS_OAM1`)
   - Oracle Access Manager Policy Manager Managed Server (`WLS_AMA1`)
   - Oracle Mobile Security Manager Managed Server (`WLS_MSM1`)
2. Verify the Oracle WebLogic Server Administration Console. If the installation and configuration are successful, this console shows the Administration Server in running mode.
3. Log in to the Administration Console for Oracle Access Management using the following 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. Log in as the Oracle Access Manager administrator user (`IDSTORE_OAMADMINUSER`) you created in Section 10.6, "Preparing Your LDAP Directory as the Identity Store." Note that you must have Administrator's role and privileges.
4. Log in to the Oracle Access Manager Policy Manager Console using the following URL:

   `http://`*`oam_policy_mgr_host`*`:`*`oam_policy_mgr_port`*`/access`

   When you access the Policy Manager Console running on the Policy Manager Server, you are prompted to enter a user name and password. Log in as the Oracle Access Manager administrator user (`IDSTORE_OAMADMINUSER`) you created in Section 10.6, "Preparing Your LDAP Directory as the Identity Store."

   For more information about the Policy Manager Server, see the "Unified Access Console" topic in *Administering Oracle Mobile Security Suite*.
5. From the Policy Manager Console, click the **Configuration** tab in the top right corner.
6. In the Configuration Launch Pad, click **Available Services**.
7. On the Available Services page, ensure that the status of **Mobile Security Service** has a green check mark. If not, click **Enable Service** next to **Mobile Security Service** to enable the status of **Mobile Security Service**.

   After you enable **Mobile Security Service**, you can access the Mobile Security Manager pages on the Policy Manager Console

8. To access the Mobile Security Manager console pages, click the **Mobile Security** tab in the top right corner.

   The Mobile Security Launch Pad opens. Under **Mobile Security Manager**, click **View** to choose from the Mobile Security Manager console pages in the menu.

   For more information about these pages, see "Working With the Mobile Security Manager Console Pages" in *Administering Oracle Mobile Security Suite*.

10.11 Optional: Creating Additional Administrator Groups After Configuration

After the installation and configuration process, specific users, groups, and roles for your Oracle Mobile Security Suite deployment have been set up in the LDAP directory, by default. If you want to create and add additional administrator groups for Oracle Access Manager and Oracle Mobile Security Suite administration, see to the following topics:

- Creating Additional System Administrator Groups After Configuration
- Creating Help Desk Administrator Groups After Configuration

10.11.1 Creating Additional System Administrator Groups After Configuration

After configuration, the Oracle Access Manager administrator group, `OAM11G_IDSTORE_ROLE_SECURITY_ADMIN`, is configured as the default administrator group that has administrator privileges over both Oracle Access Manager and Oracle Mobile Security Suite.

To assign full Oracle Access Manager and Oracle Mobile Security Suite administrator privileges to an additional LDAP group:

1. Create a group in the LDAP directory or use an existing group that you have already created.
2. Log in to the Policy Manager Console as the Oracle Access Manager administrator user, `IDSTORE_OAMADMINUSER`.

   `http://`*`oam_policy_mgr_host`*`:`*`oam_policy_mgr_port`*`/access`

3. Grant Oracle Access Manager administrator group privileges to the new group.
   a. Click the **Configuration** tab in the top right corner.
   b. In the Configuration Launch Pad, click **Administration**.
   c. On the Administration page, click **Grant**.
   d. Enter the name of the group in the **Name** field and click **Search**.
   e. In the search results, select the name of the group.
   f. For **Role**, select **System Administrator**.
   g. Click **Add selected**.
4. If Oracle Mobile Security Manager configuration, as described in Section 10.8, "Configuring Oracle Mobile Security Manager," is already complete, then this new group will be automatically added as an Oracle Mobile Security Suite administrator group as well.

However, if Oracle Mobile Security Manager is not yet configured, then you must manually assign the group to be an Oracle Mobile Security Suite administrator group. To do this, perform the following steps:

a. Navigate to the Configuration Launch Pad in the **Configuration** tab.

b. Under **Settings**, click **View** and select **Mobile Security Manager Settings**.

c. On the Mobile Security Settings page, select **Identity Store Settings**.

d. Under **System Admin Groups**, click **Add**.

e. In the **Group Name** field, enter the name of the LDAP group to be added as an Oracle Mobile Security Suite administrator group.

f. Click **Apply**.

5. Grant WebLogic administrator privileges to the new administrator group.

   To do this, you can either make this group a member of the WebLogic Server administrator group, `IDSTORE_WLSADMINGROUP`.

   OR

   You can grant WebLogic administrator privileges through the WebLogic Server Administration Console as follows:

   a. Log in to the WebLogic Server Administration Console.

   b. Click **Security Realms** from the **Domain Structure** menu.

   c. Click **myrealm** in the Realms table.

   d. Click the **Roles and Policies** tab.

   e. Expand the **Global Roles** entry in the Roles table. This brings up the entry for Roles.

   f. Click **Roles** under the **Global Roles** entry.

   g. Click the **Admin** role in the Global Roles table.

   h. Under **Role Conditions**, click **Add Conditions**.

   i. Select **Group** from the predicate list and click **Next**.

   j. In the **Group Argument Name** field, enter the name of the new group.

      Click **Add**.

   k. Click **Finish**.

      Role Conditions now shows the new administrator group as an entry.

   l. Click **Save**, and then restart the Administration Server and Managed Servers.

10.11.2 Creating Help Desk Administrator Groups After Configuration

After configuration, the Oracle Mobile Security Suite help desk role, `OMSS_IDSTORE_ROLE_SECURITY_HELPDESK`, is configured as the default administrator role that provides help desk administrative privileges for some Oracle Mobile Security Suite operations. A help desk role is associated with a directory group, which has limited administrator privileges. This group has to be created manually.

To assign help desk privileges to a LDAP group:

1. Create a group in the LDAP directory or use an existing group that you have already created.

2. Log in to the Policy Manager Console as the Oracle Access Manager administrator user, `IDSTORE_OAMADMINUSER`.

   `http://oam_policy_mgr_host:oam_policy_mgr_port/access`

3. Grant Oracle Access Manager help desk administrator privileges to the group.
   a. Click the **Configuration** tab in the top right corner.
   b. In the Configuration Launch Pad, click **Administration**.
   c. On the Administration page, click **Grant**.
   d. Enter the name of the group in the **Name** field and click **Search**.
   e. In the search results, select the name of the group.
   f. For **Role**, select **Help Desk Administrator**.
   g. Click **Add selected**.
4. If Oracle Mobile Security Manager configuration, as described in Section 10.8, "Configuring Oracle Mobile Security Manager," is already complete, then this new group will be automatically added as an Oracle Mobile Security Suite help desk administrator group as well.

   However, if Oracle Mobile Security Manager is not yet configured, then you must manually assign the group to be an Oracle Mobile Security Suite help desk group. To do this, perform the following steps:
   a. Navigate to the Configuration Launch Pad in the **Configuration** tab.
   b. Under **Settings**, click **View** and select **Mobile Security Manager Settings**.
   c. On the Mobile Security Settings page, select **Identity Store Settings**.
   d. Under **Helpdesk Groups**, click **Add**.
   e. In the **Group Name** field, enter the name of the LDAP group to be added as an Oracle Mobile Security Suite help desk administrator group.
   f. Click **Apply**.

10.12 Installing Oracle Mobile Security Access Server

After installing and configuring Oracle Mobile Security Manager with Oracle Access Manager, you need to install and configure the Oracle Mobile Security Access Server component. This document does not cover the information for installing Mobile Security Access Server. To install Mobile Security Access Server, follow the instructions in *Installing Oracle Mobile Security Access Server*.

10.13 Getting Started with Oracle Mobile Security Suite After Installation

After installing Oracle Mobile Security Suite, refer to the following links to get started working with the Oracle Mobile Security Suite components:

- *Administering Oracle Mobile Security Suite*
- *Administering Mobile Security Access Server*

11

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

This chapter explains how to configure the database security store for an Oracle Identity and Access Management domain.

This chapter includes the following topics:

11.1 Overview

After configuring the WebLogic Server Administration Domain for Oracle Identity and Access Management components and before starting the Oracle WebLogic Administration Server, you must run the `configureSecurityStore.py` script to configure the Database Security Store as it is the only security store type supported by Oracle Identity and Access Management 11*g* Release 2 (11.1.2.3.0).

The `configureSecurityStore.py` script is located in the *`IAM_HOME`*`\common\tools` directory (on Windows) and in the *`IAM_HOME`*`/common/tools` directory (on Linux or UNIX). 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 Linux or UNIX:

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

Table 11–1 describes the parameters that you can specify on the command line.

Table 11–1 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.
`-c configmode`	The configuration mode of the domain. When configuring Database Security Store this value must be specified as `IAM`. **Special Instructions for Oracle Entitlements Server Installation:** If you are an Oracle Entitlements Server user, then the `-c` parameter is optional. In this case, the default value is `None`. **Note:** If `-c config` option is specified, the Oracle Entitlements Server Administration Server will be configured in mixed mode, and it can only distribute policies to Security Modules in non-controlled mode and controlled pull mode. For example: If the Oracle Entitlements Server Administration Server is deployed in the domain where other Oracle Identity and Access Management components (such as, Oracle Identity Manager, Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Privileged Account Manager) are deployed, then the domain is configured in mixed mode. In this case, the Oracle Entitlements Server 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 Oracle Entitlements Server Security Modules. If `-c config` option is not specified, Oracle Entitlements Server Administration Server will be configured in non-controlled mode, and it can distribute policies to Security Modules in controlled push mode. For example: If you want to use Oracle Entitlements Server Administration Server to manage custom applications that are protected by Oracle Entitlements Server Security Modules, then the Oracle Entitlements Server 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.

Table 11–1 (Cont.) Database Security Store Configuration Parameters

Parameter	Description
`-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.

11.2 Before Configuring Database Security Store

Each Oracle Identity and Access Management 11*g* Release 2 (11.1.2.3.0) 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 (11.1.2.3.0) domain, you must identify the products to be configured in a single-domain scenario or in a multiple-domain scenario.

11.3 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 DOMAIN_HOME -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
\u01\oracle\admin\domains\base_domain -c IAM -p welcome1 -m create
```

On Linux or UNIX:

```
MW_HOME/oracle_common/common/bin/wlst.sh IAM_
HOME/common/tools/configureSecurityStore.py -d DOMAIN_HOME -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
/u01/oracle/admin/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=keyFile
Path,
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 DOMAIN_HOME
   -c IAM -p opss_schema_password -m join -k keyfilepath -w keyfilepassword
   ```

For example:

```
MW_HOME\oracle_common\common\bin\wlst.cmd
exportEncryptionKey(jpsConfigFile="\\u01\\oracle\\admin\\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 \u01\oracle\admin\domains\base_
domain -c IAM -p welcome1 -m join -k myDir -w password
```

On Linux or 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.sh
   exportEncryptionKey(jpsConfigFile=jpsConfigFile,
   keyFilePath=keyFilePath, keyFilePassword=keyFilePassword)
   ```

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

   ```
   MW_HOME/oracle_common/common/bin/wlst.sh IAM_
   ```

```
HOME/common/tools/configureSecurityStore.py -d DOMAIN_HOME
-c IAM -p opss_schema_password -m join -k keyfilepath -w keyfilepassword
```

For example:

```
MW_HOME/oracle_common/common/bin/wlst.sh
exportEncryptionKey(jpsConfigFile="/u01/oracle/admin/domains/base_
domain/config/fmwconfig/jps-config.xml",
keyFilePath="myDir" , keyFilePassword="password")

MW_HOME/oracle_common/common/bin/wlst.sh IAM_
HOME/common/tools/configureSecurityStore.py -d /u01/oracle/admin/domains/base_
domain
-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 DOMAIN_HOME -m
validate
```

For example:

```
MW_HOME\oracle_common\common\bin\wlst.cmd IAM_
HOME\common\tools\configureSecurityStore.py -d
\u01\oracle\admin\domains\base_domain -m validate
```

On Linux or UNIX:

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

For example:

```
MW_HOME/oracle_common/common/bin/wlst.sh IAM_
HOME/common/tools/configureSecurityStore.py -d
/u01/oracle/admin/domains/base_domain -m validate
```

11.4 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 Scenarios for Oracle Identity and Access Management Products in Different Domains

11.4.1 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 4–1, " 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
   \u01\oracle\admin\domains\oim_dom -c IAM -p welcome1 -m create
   ```

   On Linux or UNIX:

   ```
   MW_HOME/oracle_common/common/bin/wlst.sh IAM_
   HOME/common/tools/configureSecurityStore.py -d
   /u01/oracle/admin/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.

11.4.2 Example Scenarios 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 create a new 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 with different Database Security Stores**

  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 4–1, " 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 for the Oracle Identity Manager domain as follows:

     On Windows:

```
MW_HOME\oracle_common\common\bin\wlst.cmd IAM_
HOME\common\tools\configureSecurityStore.py -d
\u01\oracle\admin\domains\oim_dom -c IAM -p welcome1 -m create
```

On Linux or UNIX:

```
MW_HOME/oracle_common/common/bin/wlst.sh IAM_
HOME/common/tools/configureSecurityStore.py -d
/u01/oracle/admin/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 5–1, " Configuration Flow for Oracle Access Management".

   After creating a new WebLogic domain for Oracle Access Management, run the `configureSecurityStore.py` script to configure a separate Database Security Store for the Oracle Access Management domain as follows:

   On Windows:

```
MW_HOME\oracle_common\common\bin\wlst.cmd IAM_
HOME\common\tools\configureSecurityStore.py -d
\u01\oracle\admin\domains\oam_dom -c IAM -p welcome1 -m create
```

   On Linux or UNIX:

```
MW_HOME/oracle_common/common/bin/wlst.sh IAM_
HOME/common/tools/configureSecurityStore.py -d
/u01/oracle/admin/domains/oam_dom -c IAM -p welcome1 -m create
```

- **Scenario 2: Extend the Oracle Access Management Domain and its previously created 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 Management domain.

12

Verifying Your Environment Using the Environment Health Check Utility

After installing and configuring Oracle Identity and Access Management, Oracle recommends you run the Oracle Identity and Access Environment Health Check Utility to verify that your environment has been configured successfully.

For more information, see the following topics:

- Running the Environment Health Check Utility After Configuration
- Running the Environment Health Check Utility to Verify Your Installation and Configuration
- Running the Environment Health Check Utility to Verify Oracle Identity Manager
- Running the Environment Health Check Utility to Verify Oracle Access Manager

12.1 Running the Environment Health Check Utility After Configuration

The Environment Health Check Utility is a tool available from the *IAM_HOME*/healthcheck directory that you can use to verify various configurations and perform validation checks against your Oracle Identity and Access Management setup. These checks help you verify that your environment has been installed and configured successfully. When you run the Health Check Utility, the utility retrieves data from your environment, uses the data to run a set of validation checks, and generates a report that provides detailed information about any issues the utility finds for each of the items it checks.

To run the utility, you specify a manifest file, which is used to group together specific validation checks and call plug-ins to run the various checks. To run general post-installation checks to verify general post-installation requirements, see Section 12.2.

For Oracle Identity Manager and Oracle Access Manager, it is also recommended you run the utility to perform component validation checks to ensure these components are set up correctly. To run component-specific checks for Oracle Identity Manager and Oracle Access Manager, see Section 12.3 and Section 12.4, respectively.

For more information about the Environment Health Check Utility, see "Understanding the Oracle Identity and Access Environment Health Check Utility" in *Verifying Your Oracle Identity and Access Management Environment*.

Note: *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 Privileged Account Manager, Oracle Access Management Mobile and Social, and Oracle Mobile Security Suite.

12.2 Running the Environment Health Check Utility to Verify Your Installation and Configuration

After installing and configuring Oracle Identity and Access Management, it is recommended you run the Health Check Utility to verify that your environment meets general post-installation requirements. To do this, you use the *IAM_HOME*/healthcheck/config/PostInstallChecks.xml manifest file to run the appropriate post-installation checks.

Note: For more information about these checks performed by the Health Check Utility, see "PostInstallChecks.xml" in *Verifying Your Oracle Identity and Access Management Environment*

To ensure your environment has been installed and configured successfully, perform the following steps to run general post-installation checks:

1. Open the idmhc.properties file in the *IAM_HOME*/healthcheck/bin directory.
2. Set values for the necessary properties in this file to reflect your Oracle Identity and Access Management environment.

   For more information on how to update and use this file, see "Understanding the idmhc.properties File of the Health Check Utility" in *Verifying Your Oracle Identity and Access Management Environment*.
3. Set the JAVA_HOME environment variable to the full path of the JDK directory.
4. Change directory to the *IAM_HOME*/healthcheck/bin directory (on Linux or UNIX) or *IAM_HOME*\healthcheck\bin directory (on Windows).

   On Linux or UNIX:

   ```
   cd IAM_HOME/healthcheck/bin
   ```

   On Windows:

   ```
   cd IAM_HOME\healthcheck\bin
   ```
5. Run the following command to perform post-installation validation checks:

   On Linux or UNIX:

   ```
   idmhc.sh -manifest IAM_HOME/healthcheck/config/PostInstallChecks.xml
   ```

   On Windows:

   ```
   idmhc.bat -manifest IAM_HOME\healthcheck\config\PostInstallChecks.xml
   ```
6. If any health checks fail, refer to the output in the Health Check Utility log files and reports to find the corrective actions. Note that the log file location will be printed on the screen after the utility is executed.

The reports provide the status of each check and a list of corrective actions for any checks that fail validation. You can manually fix the issues and rerun the utility any number of times to ensure all checks are successful. For more information about the log files and reports, see "Analyzing Health Check Reports" in *Verifying Your Oracle Identity and Access Management Environment*.

12.3 Running the Environment Health Check Utility to Verify Oracle Identity Manager

After configuring Oracle Identity Manager, it is recommended you run the Health Check Utility to verify your Oracle Identity Manager configuration. To do this, you use the *IAM_HOME*/healthcheck/config/PostInstallChecks_oim.xml manifest file to run the appropriate Oracle Identity Manager checks.

Note: For more information about the Oracle Identity Manager checks performed by the Health Check Utility, see "PostInstallChecks_oim.xml (Oracle Identity Manager)" in *Verifying Your Oracle Identity and Access Management Environment*.

To ensure Oracle Identity Manager has been configured successfully, perform the following steps to run Oracle Identity Manager validation checks:

1. Open the idmhc.properties file in the *IAM_HOME*/healthcheck/bin directory.
2. Set values for the necessary properties in this file to reflect your Oracle Identity and Access Management environment.

   For more information on how to update and use this file, see "Understanding the idmhc.properties File of the Health Check Utility" in *Verifying Your Oracle Identity and Access Management Environment*.
3. Set the JAVA_HOME environment variable to the full path of the JDK directory.
4. Change directory to the *IAM_HOME*/healthcheck/bin directory (on Linux or UNIX) or *IAM_HOME*\healthcheck\bin directory (on Windows).

   On Linux or UNIX:

   ```
   cd IAM_HOME/healthcheck/bin
   ```

   On Windows:

   ```
   cd IAM_HOME\healthcheck\bin
   ```
5. Run the following command to perform Oracle Identity Manager validation checks:

   On Linux or UNIX:

   ```
   idmhc.sh -manifest IAM_HOME/healthcheck/config/PostInstallChecks_oim.xml
   ```

   On Windows:

   ```
   idmhc.bat -manifest IAM_HOME\healthcheck\config\PostInstallChecks_oim.xml
   ```
6. If any health checks fail, refer to the output in the Health Check Utility log files and reports to find the corrective actions. Note that the log file location will be printed on the screen after the utility is executed.

The reports provide the status of each check and a list of corrective actions for any checks that fail validation. You can manually fix the issues and rerun the utility any number of times to ensure all checks are successful. For more information about the log files and reports, see "Analyzing Health Check Reports" in *Verifying Your Oracle Identity and Access Management Environment*.

12.4 Running the Environment Health Check Utility to Verify Oracle Access Manager

After configuring Oracle Access Manager, it is recommended you run the Health Check Utility to verify your Oracle Access Manager configuration. To do this, you use the *IAM_HOME*/healthcheck/config/PostInstallChecks_oam.xml manifest file to run the appropriate Oracle Access Manager checks.

Note: For more information about the Oracle Access Manager checks performed by the Health Check Utility, see "PostInstallChecks_oam.xml (Oracle Access Manager)" in *Verifying Your Oracle Identity and Access Management Environment*.

To ensure Oracle Access Manager has been configured successfully, perform the following steps to run Oracle Access Manager validation checks:

1. Open the idmhc.properties file in the *IAM_HOME*/healthcheck/bin directory.
2. Set values for the necessary properties in this file to reflect your Oracle Identity and Access Management environment.

   For more information on how to update and use this file, see "Understanding the idmhc.properties File of the Health Check Utility" in *Verifying Your Oracle Identity and Access Management Environment*.
3. Set the JAVA_HOME environment variable to the full path of the JDK directory.
4. Change directory to the *IAM_HOME*/healthcheck/bin directory (on Linux or UNIX) or *IAM_HOME*\healthcheck\bin directory (on Windows).

   On Linux or UNIX:

   ```
   cd IAM_HOME/healthcheck/bin
   ```

   On Windows:

   ```
   cd IAM_HOME\healthcheck\bin
   ```
5. Run the following command to perform Oracle Access Manager validation checks:

   On Linux or UNIX:

   ```
   idmhc.sh -manifest IAM_HOME/healthcheck/config/PostInstallChecks_oam.xml
   ```

   On Windows:

   ```
   idmhc.bat -manifest IAM_HOME\healthcheck\config\PostInstallChecks_oam.xml
   ```
6. If any health checks fail, refer to the output in the Health Check Utility log files and reports to find the corrective actions. Note that the log file location will be printed on the screen after the utility is executed.

The reports provide the status of each check and a list of corrective actions for any checks that fail validation. You can manually fix the issues and rerun the utility any number of times to ensure all checks are successful. For more information about the log files and reports, see "Analyzing Health Check Reports" in *Verifying Your Oracle Identity and Access Management Environment*.

13

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.

> **Note:** This chapter describes life cycle management events that can be applied manually to Oracle Identity and Access Management products after they are installed, configured, and integrated together. This is not to be confused with the Life Cycle Management (LCM) Tools that automate the installation, configuration, patching, and upgrade of Oracle Identity and Access Management products. For more information about the LCM Tools, see the *Deployment Guide for Oracle Identity and Access Management*.

Topics include:

13.1 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 host name 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 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.

13.2 LCM for Oracle Identity Manager

Lifecycle management events for Oracle Identity Manager include:

- reassociation when the host or port changes for these components:
  - Oracle Virtual Directory
  - Oracle SOA Suite
  - MDS
- moving metadata from a test environment to a production environment

Refer to the following sources for lifecycle management procedures relating to OIM:

- "Oracle Virtual Directory Host and Port Changes" in the *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager*
- "Changing OVD Password" in the *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager*
- "SOA Host and Port Changes" in the *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager*
- "Oracle Identity Manager Database Host and Port Changes" in the *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager*
- "Oracle Identity Manager (OIM) Rewiring with Existing Oracle Adaptive Access Manager (OAAM)" in the *Oracle Fusion Middleware Developer's Guide for Oracle Adaptive Access Manager*
- "Changing Oracle Identity Manager Database Password" in the *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager*
- "Configuring LDAP Adapters" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Virtual Directory*
- "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 *Administrator's Guide*
- "Move Oracle Identity Manager to an Existing Target Environment" in the *Administrator's Guide*

13.3 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:

- "Moving OAM 11*g* from Test to Production" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager*

13.4 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:

- "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 *Administrator's Guide*
- "Move Oracle Adaptive Access Manager to an Existing Target Environment" in the *Administrator's Guide*

13.5 References

For additional information about lifecycle management in Oracle Fusion Middleware, see "Part V Advanced Administration: Expanding Your Environment" in the *Administrator's Guide*.

Part III

Appendixes

Part III contains the following appendixes:

- Appendix A, "Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0) Software Installation Screens"
- Appendix B, "Oracle Identity Manager Configuration Screens"
- Appendix C, "Starting or Stopping the Oracle Stack"
- Appendix D, "Creating Oracle Entitlement Server Schemas for Apache Derby"
- Appendix E, "Configuring the PDP Proxy Client for Web Service Security Module"
- Appendix F, "Deinstalling and Reinstalling Oracle Identity and Access Management"
- Appendix G, "Troubleshooting the Installation"
- Appendix H, "Oracle Adaptive Access Manager Partition Schema Reference"
- Appendix I, "Software Deinstallation Screens"

A

Oracle Identity and Access Management 11*g* Release 2 (11.1.2.3.0) Software Installation Screens

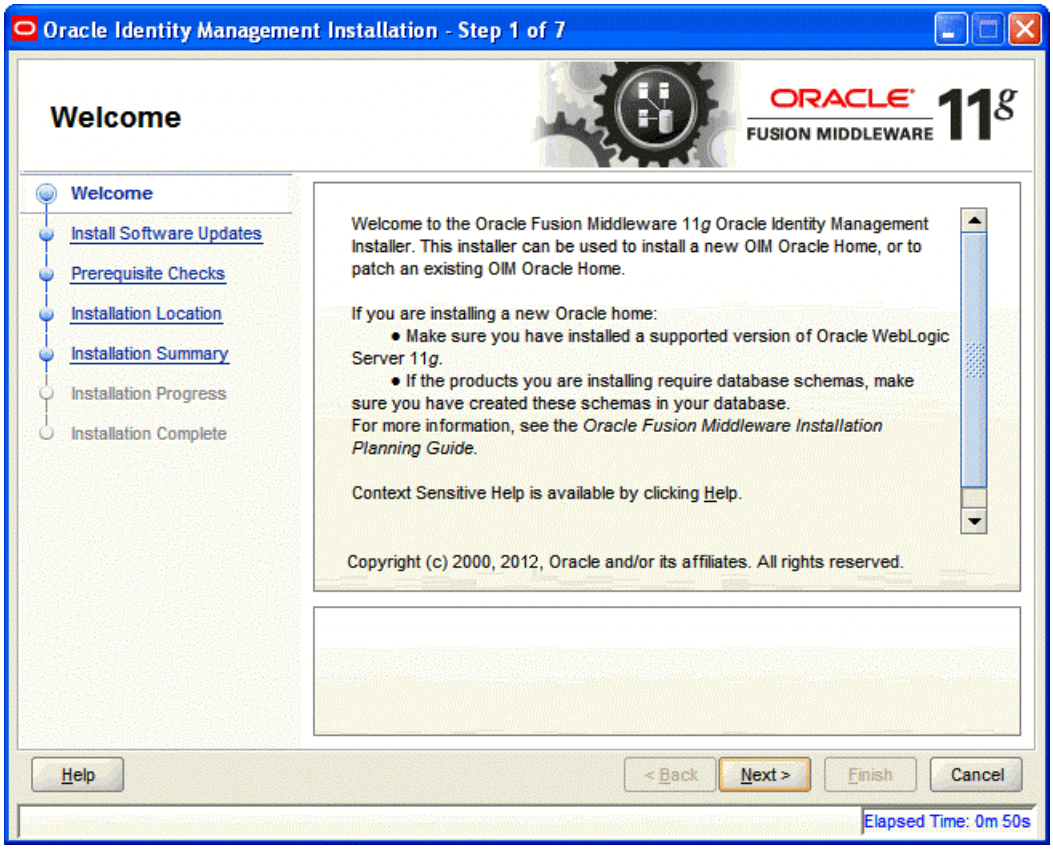
This appendix describes the screens of the Oracle Identity and Access Management 11*g* software Installation Wizard that enables you to install Oracle Identity Manager, Oracle Access Management, Oracle Adaptive Access Manager, Oracle Entitlements Server, Oracle Privileged Account Manager, Oracle Access Management Mobile and Social, and Oracle Mobile Security Suite.

It contains the following topics:

A.1 Welcome

The Welcome screen is displayed each time you start the Oracle Identity and Access Management 11*g* Installer wizard.

Figure A–1 Welcome Screen

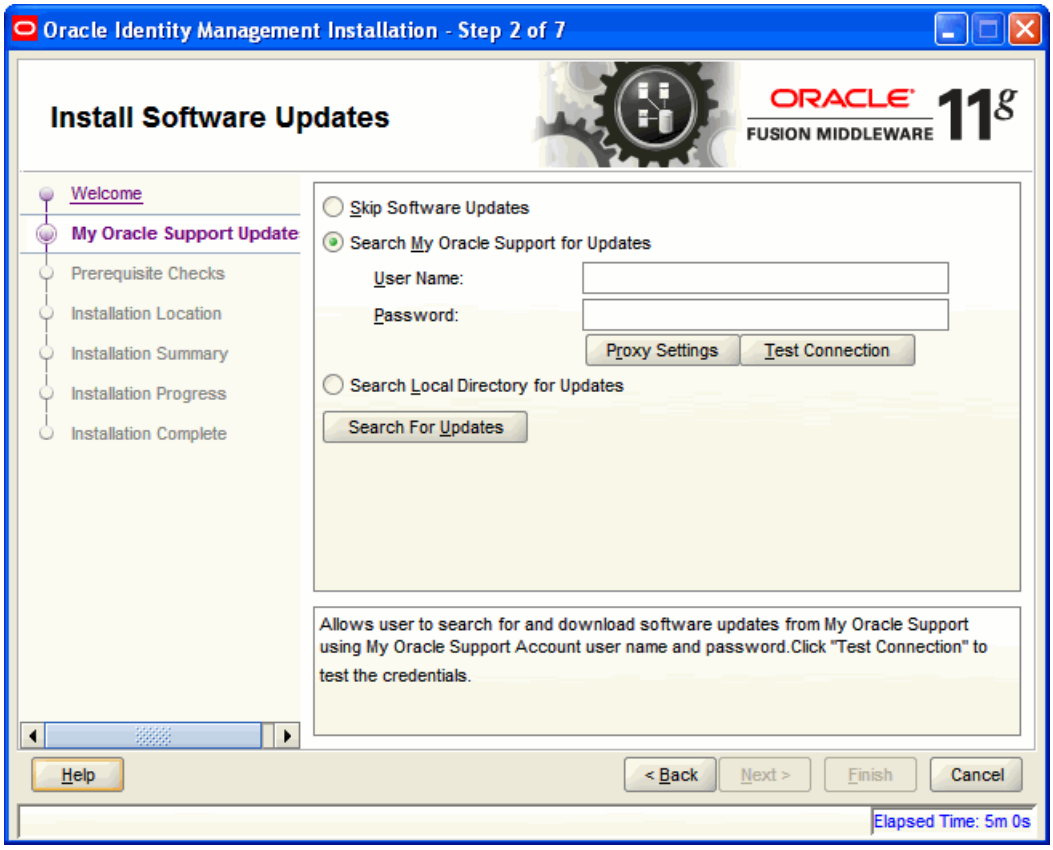


Click **Next** to continue.

A.2 Install Software Updates

This screen helps to quickly and easily search for the latest software updates, including important security updates, via your My Oracle Support account.

Figure A–2 Install Software Updates

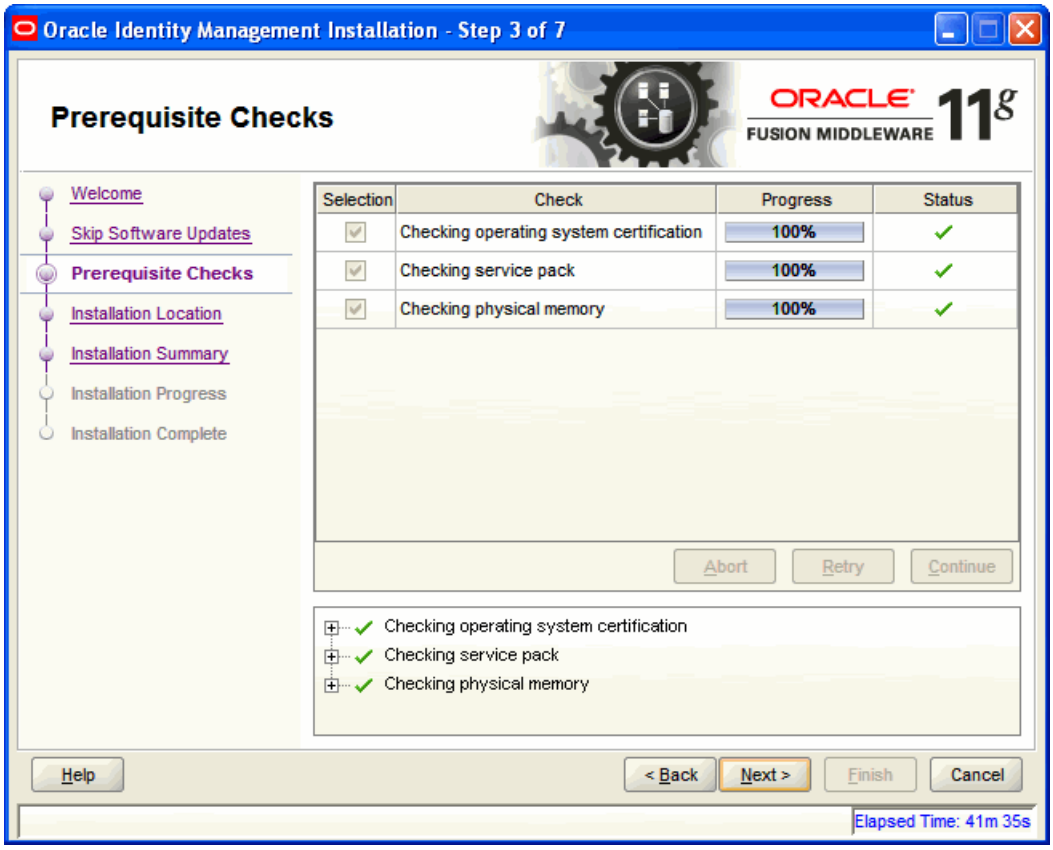


A.3 Prerequisite Checks

The installation program ensures that you have a certified version, the correct software packages, sufficient space and memory to perform the operations that you have selected. If any issues are detected, errors appear on this page.

The following example screen applies to Windows operating systems only.

Figure A–3 Prerequisite Checks Screen



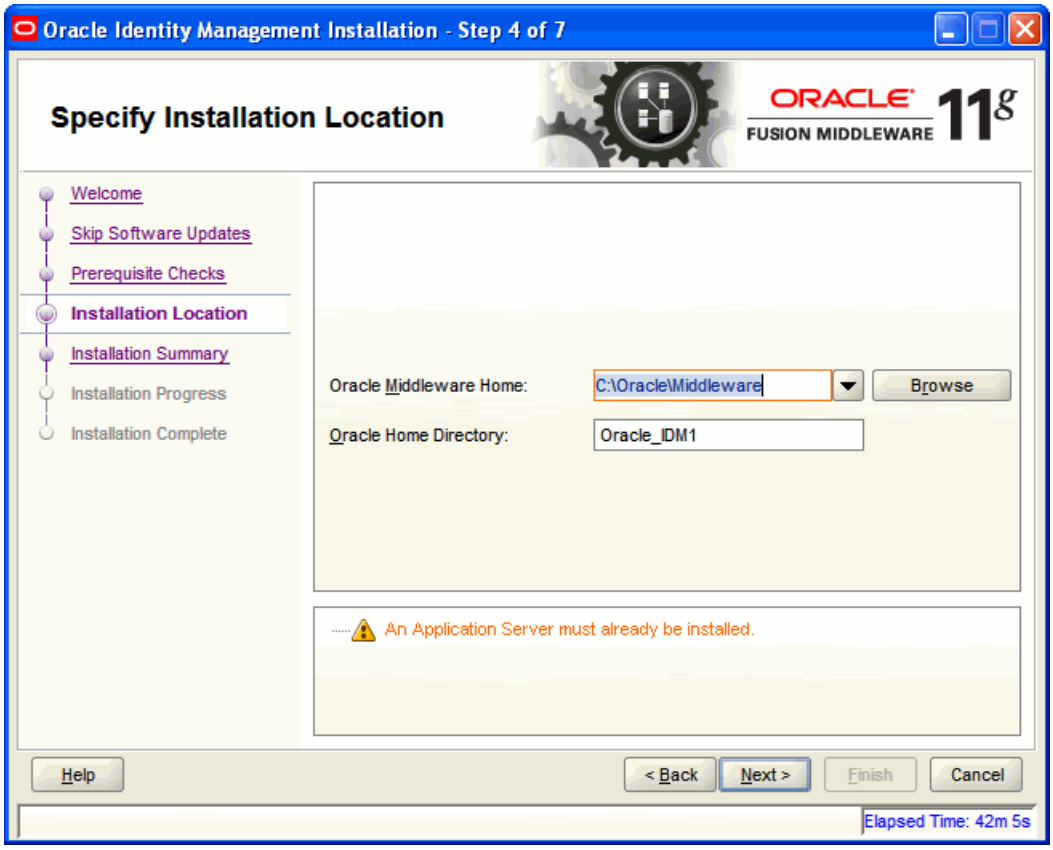
On this screen, you can select to **Abort**, **Retry**, or **Continue** with the installation.

If all the prerequisite checks pass inspection, click **Next** to continue.

A.4 Specify Installation Location

In this screen, you enter a location for the new Oracle Identity and Access Management 11*g* software being installed.

Figure A–4 Specify Installation Location Screen



Ensure that Oracle WebLogic Server is already installed on your machine. Navigate to the Oracle Fusion Middleware Home directory by clicking **Browse**. Enter a name for the new Oracle Home directory for Oracle Identity and Access Management 11g components.

If the Middleware location does not exist, you must install WebLogic Server and create a Middleware Home directory, as described in Section 3.2.6, "Installing Oracle WebLogic Server and Creating a Middleware Home", 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. This component of Oracle Identity Manager does not require a Middleware Home directory.

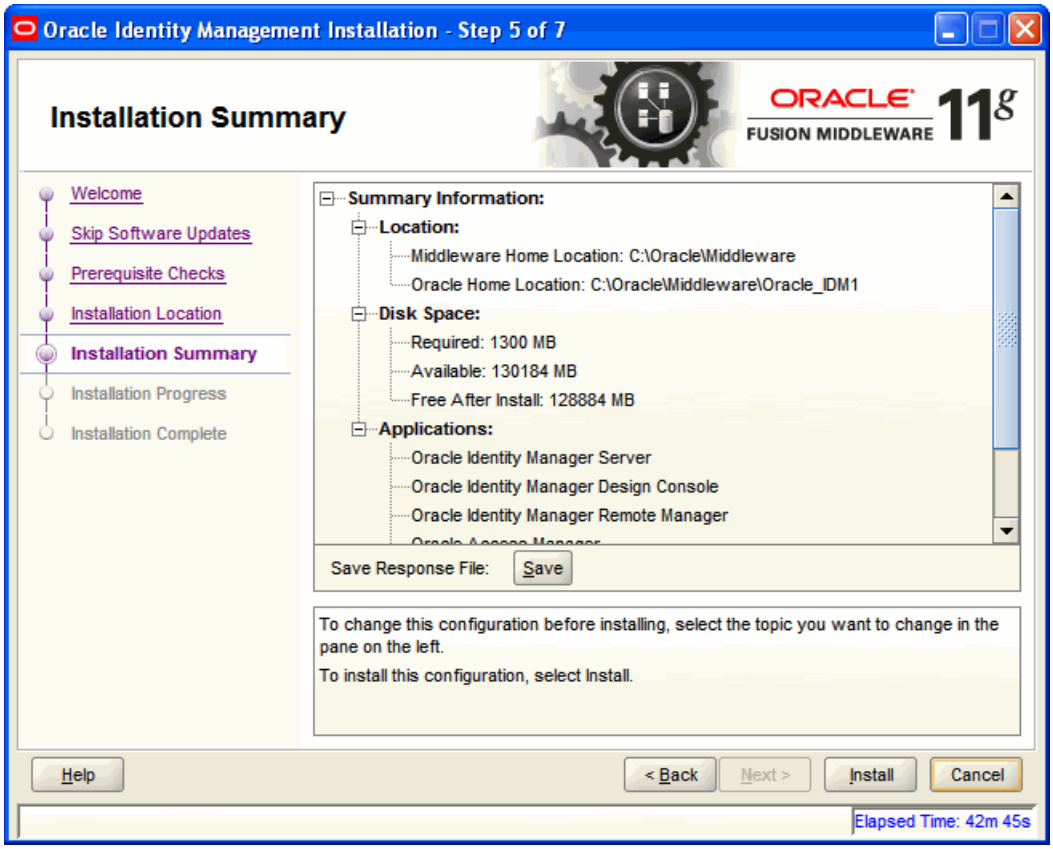
If you want to install only Oracle Identity Manager Design Console, you do not need to install Oracle WebLogic Server or create a Middleware Home directory on the machine where Design Console is being configured.

Click **Next** to continue.

A.5 Installation Summary

This screen displays a summary of your Oracle Identity and Access Management 11*g* installation.

Figure A–5 Installation Summary Screen

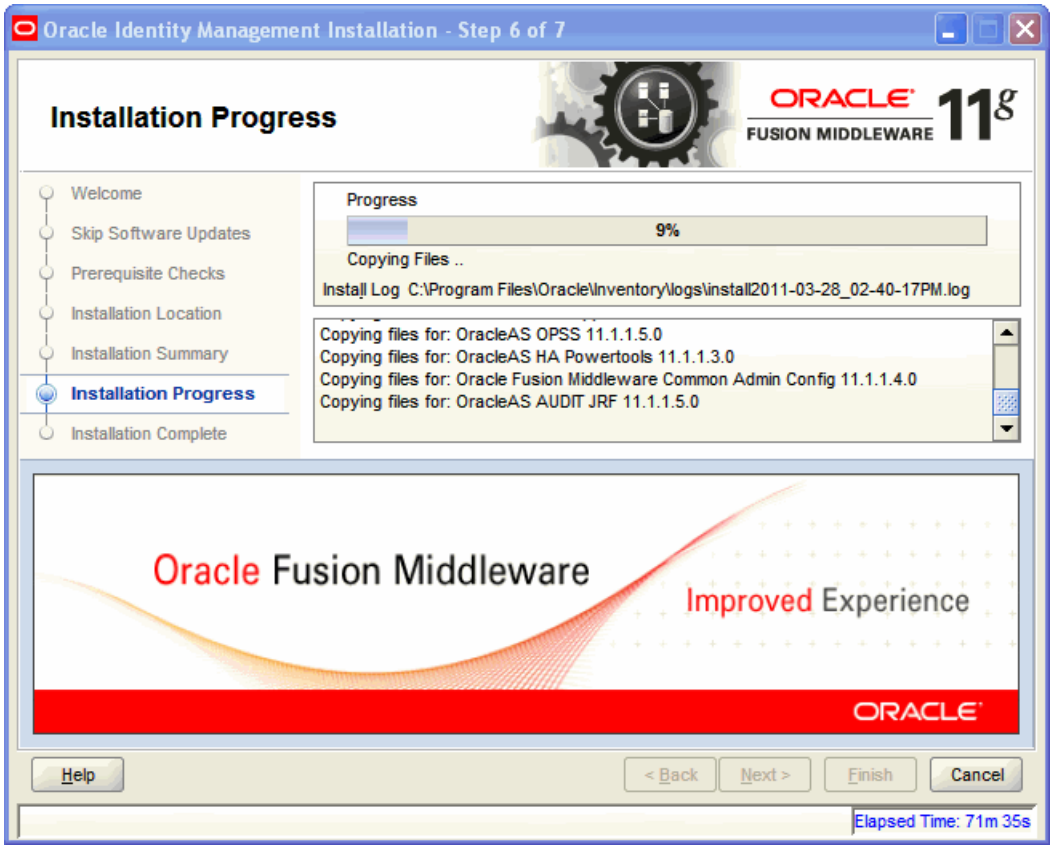


Review the contents of this screen, and click **Install** to start installing the Oracle Identity and Access Management 11*g* software.

A.6 Installation Progress

This screen displays the progress of the Oracle Identity and Access Management installation.

Figure A–6 Installation Progress Screen

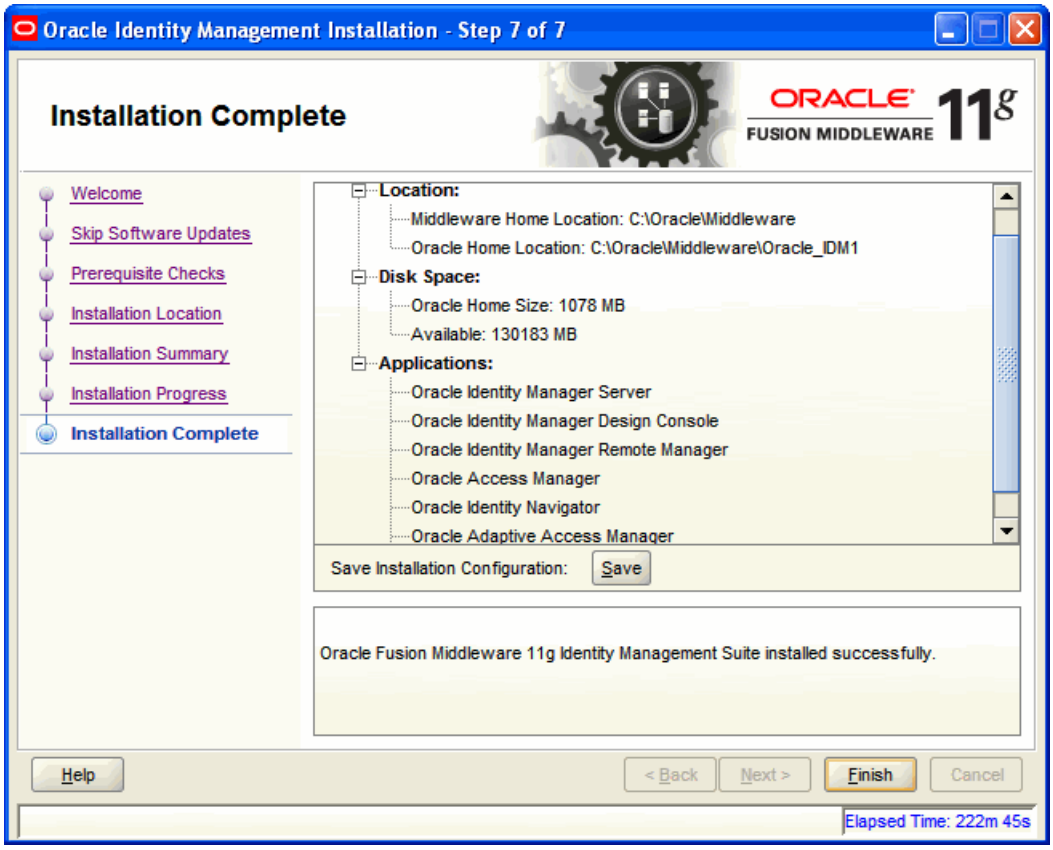


If you want to quit before the installation is completed, click **Cancel**. The installation progress indicator gives a running inventory of the files that are being installed. If you are only installing the software binaries, installation is complete after all of the binaries have been installed.

A.7 Installation Complete

This screen displays a summary of the installation parameters, such as Location, Disk Space, and Applications. To save the installation configuration in a response file, which is used to perform silent installations, click **Save**.

Figure A–7 Installation Complete Screen



Click **Finish** to complete the installation process.

B

Oracle Identity Manager Configuration Screens

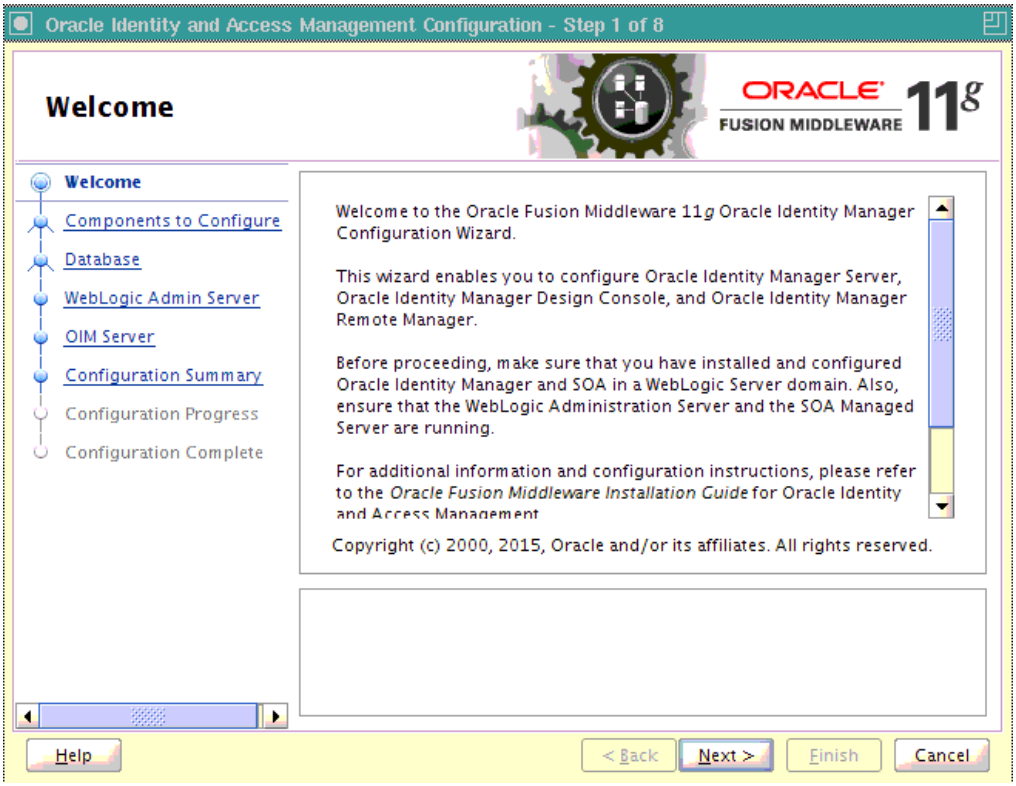
This appendix describes the screens of the Oracle Identity Manager 11*g* Configuration Wizard that enables you to configure Oracle Identity Manager Server, Oracle Identity Manager Design Console, and Oracle Identity Manager Remote Manager.

This appendix contains the following topics:

B.1 Welcome

The Welcome screen is displayed each time you start the Oracle Identity Manager Configuration Wizard.

Figure B–1 Welcome Screen



You can use the Oracle Identity Manager Configuration Wizard only once during initial setup for configuring Oracle Identity Manager Server. After configuring Oracle Identity Manager Server using this wizard, you cannot re-run this wizard to modify the configuration of Oracle Identity Manager. You must use Oracle Enterprise Manager Fusion Middleware Control to make such modifications. However, you can run this wizard on other machines, where Design Console or Remote Manager is configured, as and when needed.

Ensure that you have configured Oracle Identity Manager in a new or existing WebLogic domain before launching the Oracle Identity Manager Configuration Wizard to configure Oracle Identity Manager Server, Design Console on Windows, and Remote Manager.

If you are configuring Server, you must run this wizard on the machine where the WebLogic Administration Server is running (the Administration Server for the domain in which Oracle Identity Manager is deployed). Ensure that the Administration Server is up and running before you start configuring Oracle Identity Manager Server.

If you are configuring only Design Console, you must run this wizard on the Windows machine where Design Console should be configured. If you are configuring only Remote Manager, you must run this wizard on the machine where Remote Manager is being configured. Note that the Oracle Identity Manager Server should be configured before you can configure Design Console or Remote Manager.

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

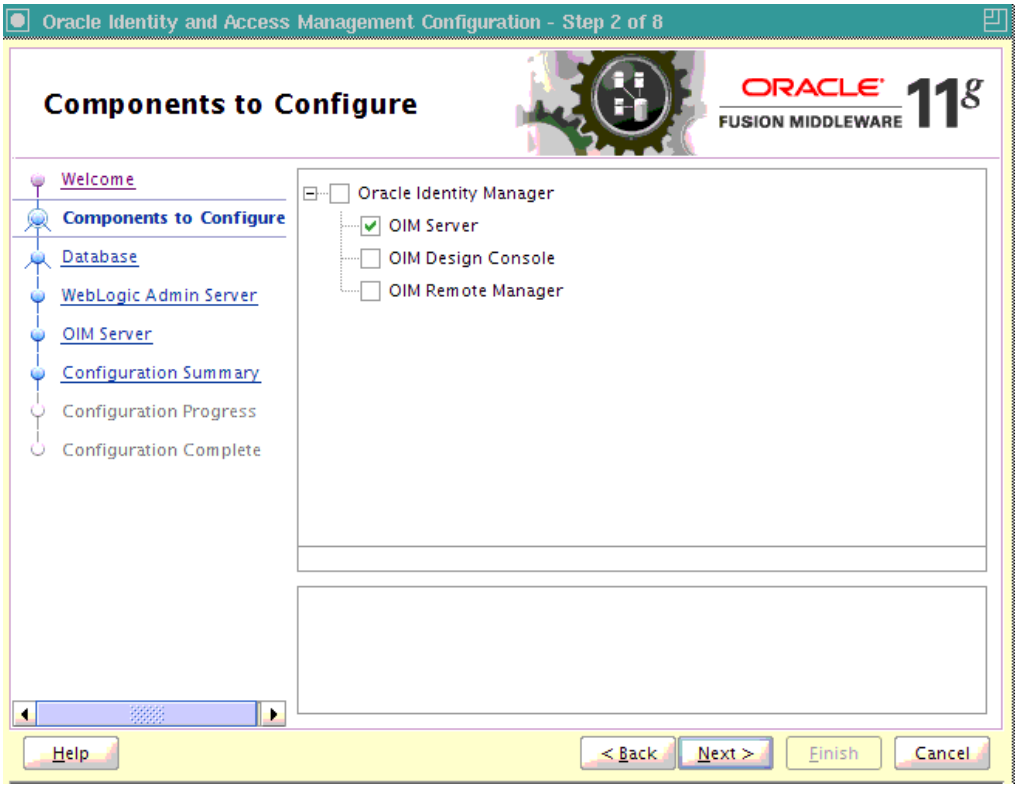


Table B–1 describes the Oracle Identity Manager components that you can choose.

Table B–1 Oracle Identity Manager Configuration Choices

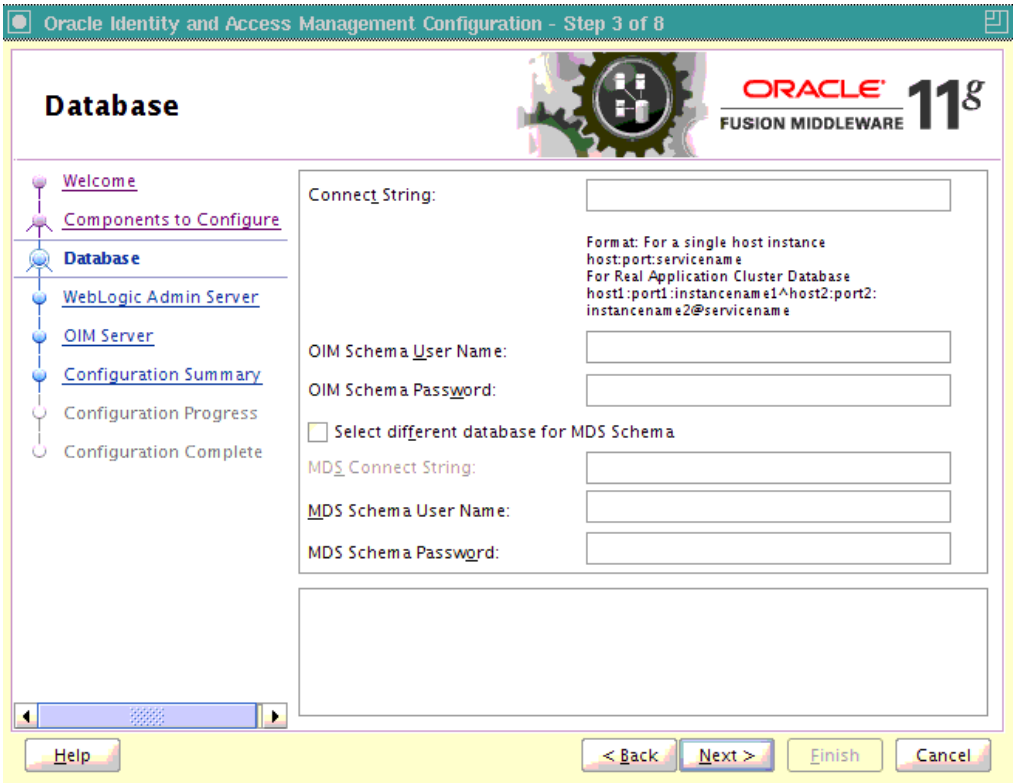
Option	Description
Oracle Identity Manager	To configure Oracle Identity Manager Server, Design Console, and Remote Manager simultaneously on the same machine, select the **Oracle Identity Manager** option.
OIM Server	To configure only Oracle Identity Manager Server, select the **OIM Server** option. 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.
OIM 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.
OIM 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 3.2.5, "Creating Database Schemas 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 2 (11.1.2), 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 2 (11.1.2), 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 2 (11.1.2), 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 2 (11.1.2), enter the password for your existing schema.

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

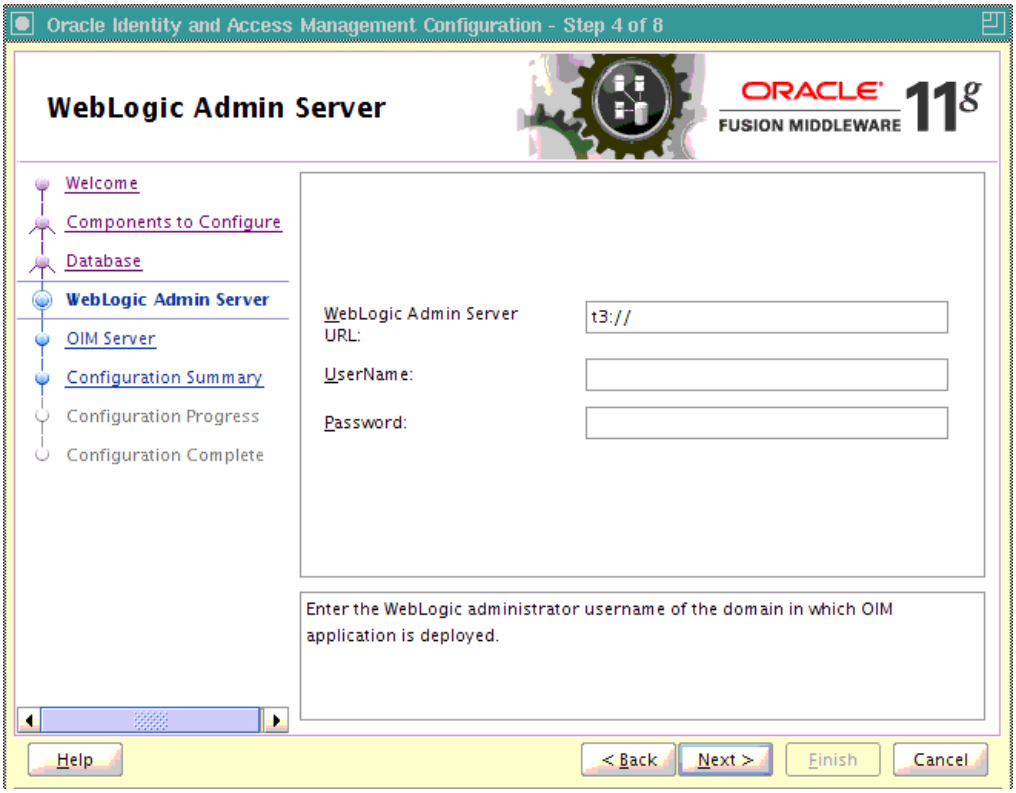


Table B–3 describes the WebLogic Admin Server information that you must specify.

Table B–3 Fields in the WebLogic Admin Server Screen

Field	Description
WebLogic Admin Server URL	Enter the t3 URL of the Administration Server for the WebLogic domain in the following format: `t3://hostname:port`
UserName	Enter the WebLogic Administrator user name.
Password	Enter the WebLogic Administrator password.

B.5 OIM Server

Use this screen to set a password for the for the system administrator (`xelsysadm`).

Figure B–5 OIM Server Screen

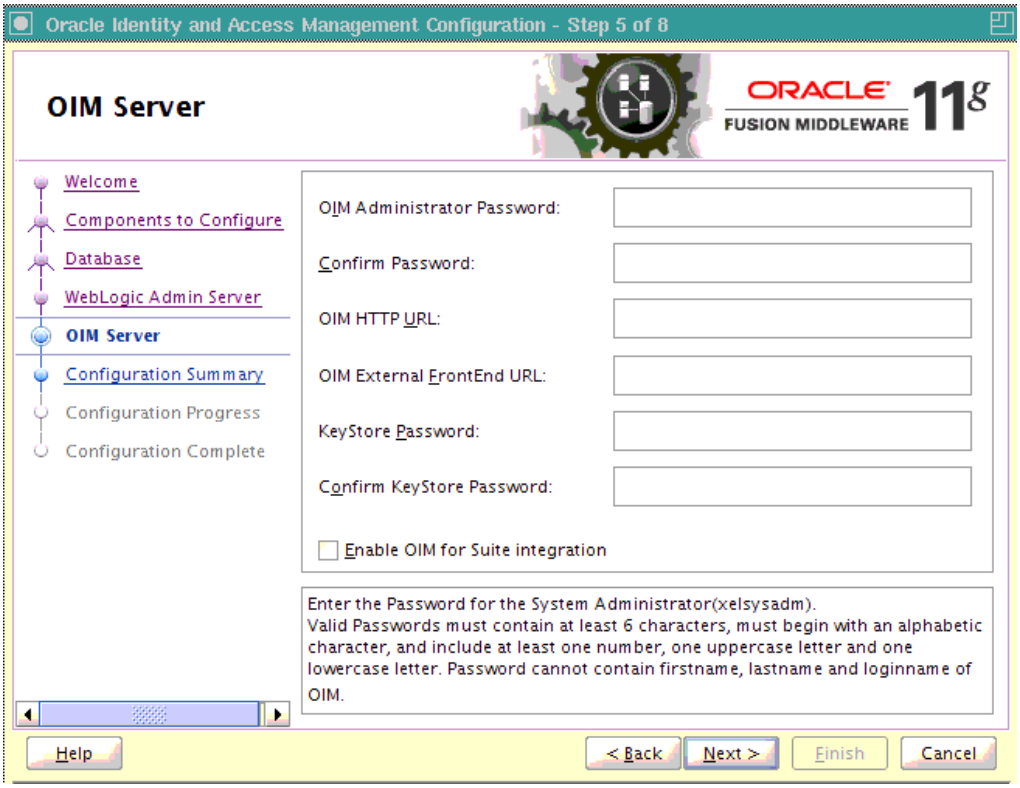


Table B–4 describes the Oracle Identity Manager Server parameters that you can configure.

Table B–4 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.

Table B–4 (Cont.) Oracle Identity Manager Server Configuration Parameters

Field Name	Description
OIM External FrontEnd URL	The OIM External Front End URL is of the format: `http(s)://<host>:<port>`. For example, `https://localhost:7070` For deployments where there is no Single Sign-On (SSO) configured but Oracle Identity Manager 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 Single Sign-On (SSO) is configured, provide the SSO URL where the Oracle Identity Manager user interface is available. For single node deployments where the Oracle Identity Manager Managed Server is not front-ended with Oracle HTTP Server, this field can be left blank.
KeyStore Password	Enter new password for the keystore. A valid password can contain 6 to 30 characters, begin with an alphabetic character, and use only alphanumeric characters and special characters like Underscore (_), Dollar ($), Pound (#). The password must contain at least one number.
Confirm KeyStore Password	Enter the new password again to confirm.
Enable OIM for Suite integration	Select the **Enable OIM for Suite integration** check box if you are planning to integrate Oracle Identity Manager with Oracle Access Manager. When you select this option, the Oracle Identity Manager Configuration Wizard configures LDAP sync to synchronize identity store information between the Oracle Identity Manager database store and the Oracle Access Manager LDAP directory service.

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 are planning to integrate Oracle Identity Manager with Oracle Access Management.

If you want to enable LDAP Sync, you must first set up LDAP Sync for Oracle Identity Manager before selecting the **Enable OIM for Suite integration** option on this screen. For information about setting up OIM-LDAP Sync, see "Completing the Prerequisites for Enabling LDAP Synchronization" and "Creating OVD Adapters" in the *Integration Guide for Oracle Identity Management Suite*. After completing the prerequisites for enabling LDAP Synchronization, select the **Enable OIM for Suite integration** option.

B.6 LDAP Server

The LDAP Server screen is displayed only if you selected **Enable OIM for Suite integration** on the OIM Server screen. In this case, you will be connecting to the LDAP server to enable synchronization of the Oracle Identity Manager roles, users, and their hierarchy between the database and the LDAP directory used for Oracle Access Manager.

In the LDAP Server screen, you should specify the authentication information for the Directory Server.

Figure B–6 LDAP Server Screen

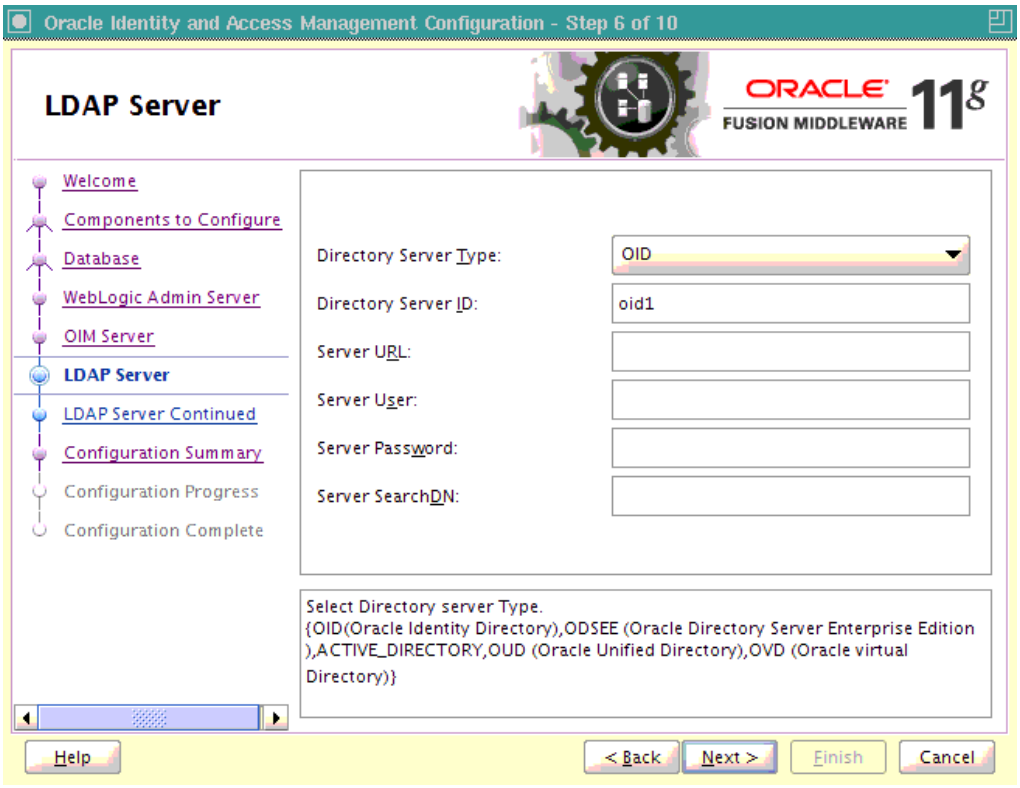


Table B–5 describes the parameters that you must specify.

Table B–5 LDAP Server Information

Field Name	Description
Directory Server Type	Select the desired Directory Server from the drop-down list. You have the following options: ▪ OID ▪ ODSEE/IPLANET ▪ OUD ▪ ACTIVE_DIRECTORY ▪ OVD
Directory Server ID	Enter the Directory Server ID.
Server URL	Enter the LDAP URL in the format: `ldap://ldap_host:ldap_port` For Microsoft Active Directory, the LDAP URL must be a SSL URL.
Server User	Enter the user name for the Directory Server administrator. For example: `cn=oimAdminUser,cn=Users,dc=example,dc=com`
Server Password	Enter the password for the Directory Server administrator.

Table B–5 (Cont.) LDAP Server Information

Field Name	Description
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.

B.7 LDAP Server Continued

This screen is a continuation of the LDAP Server screen.

Figure B–7 LDAP Server Continued Screen

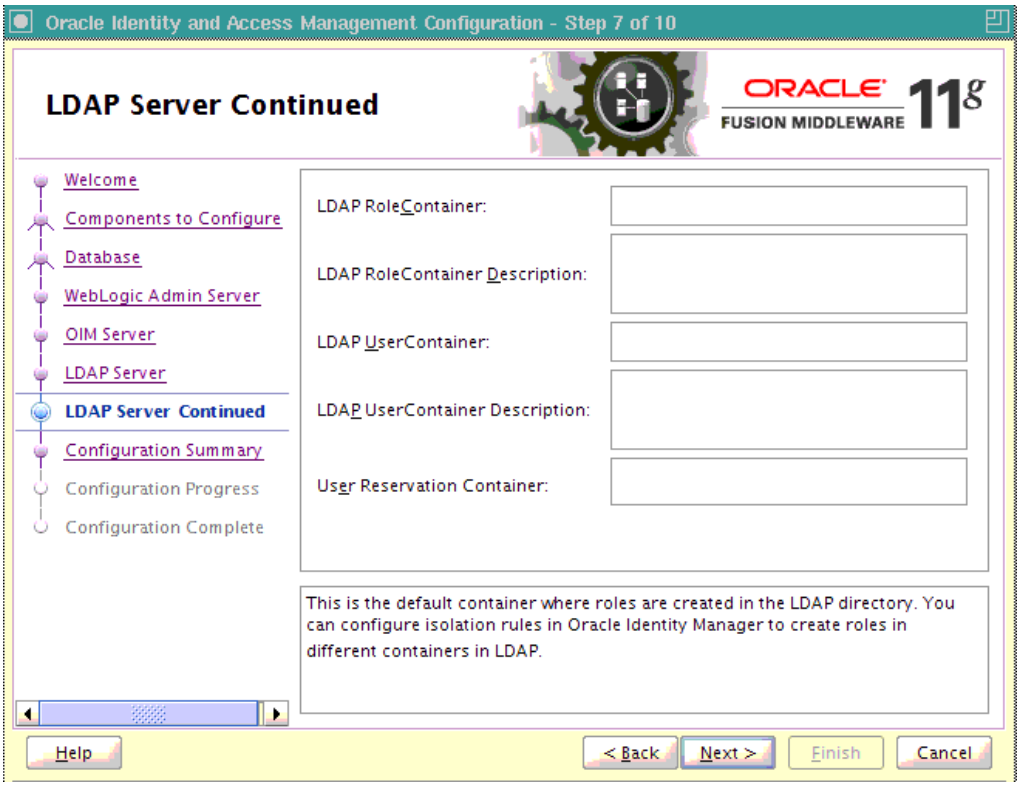


Table B–6 describes the LDAP parameters that you must specify.

Table B–6 LDAP Server Continued Information

Field Name	Description
LDAP RoleContainer	Enter a name for the container that will be used as a default container of roles in the LDAP directory.
LDAP RoleContainer Description	Type a description for the role container.
LDAP UserContainer	Enter a name for the container that will be used as a default container of users in the LDAP directory.
LDAP UserContainer Description	Type a description for the user container.

Table B–6 (Cont.) LDAP Server Continued Information

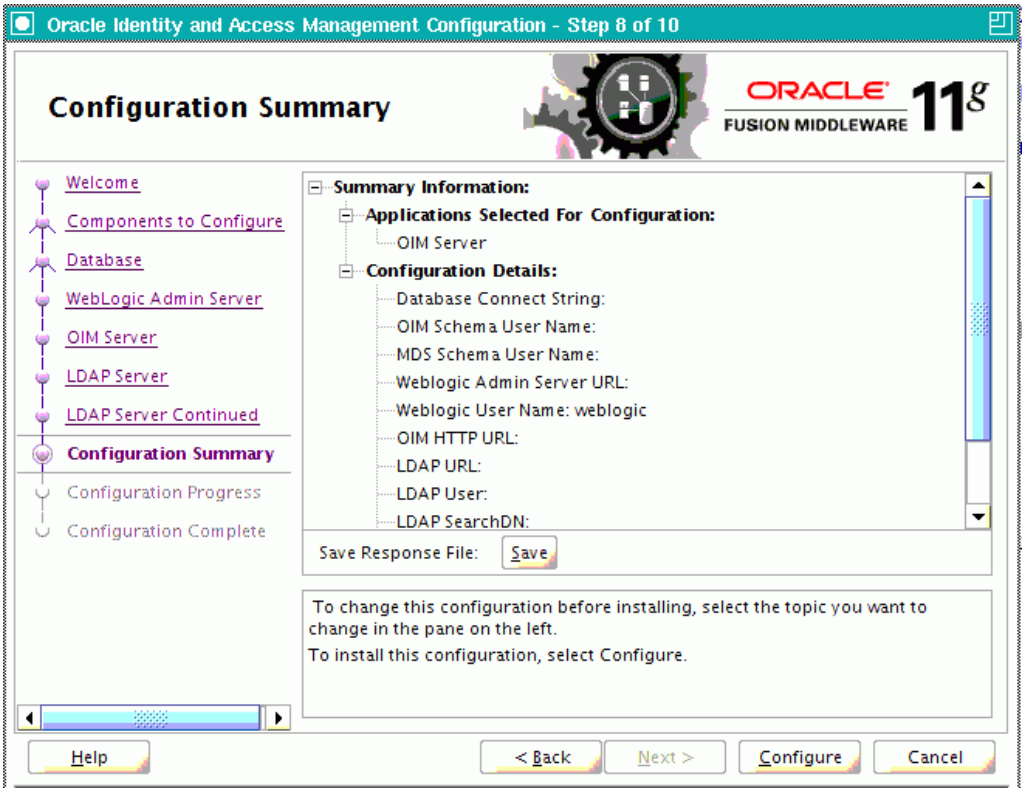
Field Name	Description
User Reservation Container	Enter a name for the container that will be used for reserving user names in the LDAP directory while their creation is being approved in Oracle Identity Manager. When the user names are approved, they are moved from the reservation container to the user container in the LDAP directory.

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_OIM1`, `WLS_MSM1`, or `WLS_OAM1`.
- 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:

Note: You must start the Node Manager, the WebLogic Administration Server, and the Managed Servers with Java Secure Socket Extension (JSSE) enabled if you have applied the following Oracle WebLogic Server patches to your Middleware home:

- 13964737 (YVDZ)
- 14174803 (IMWL)

These patches are available from My Oracle Support.

For information on how to start the Node Manager with JSSE enabled, see the "Set the Node Manager Environment Variables" topic in the *Oracle Fusion Middleware Node Manager Administrator's Guide for Oracle WebLogic Server*.

After starting Node Manager with JSSE enabled, you must start the Administration Server and Managed Servers with JSSE enabled. For more information, see the "Using the JSSE-Enabled SSL Implementation" topic in *Securing Oracle WebLogic Server*.

1. 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 Linux or 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:

      WL_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:

      WL_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.

2. To start the Administration Server, run the `startWebLogic.sh` (on Linux or UNIX operating systems) or `startWebLogic.cmd` (on Windows operating systems) script in the directory where you created your new domain (`DOMAIN_HOME`).

   On Linux or UNIX systems:

   ```
   DOMAIN_HOME/startWebLogic.sh
   ```

   On Windows systems:

   ```
   DOMAIN_HOME/startWebLogic.cmd
   ```

3. To start the Managed Servers, run the `startManagedWebLogic.sh` (on Linux or 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:

   - Oracle Identity Manager Server (`WLS_OIM1`)
   - Oracle SOA Server (`WLS_SOA1`)
   - Oracle BI Publisher Server (`WLS_BIP1`)
   - Oracle Access Management Server (`WLS_OAM1`)
   - Oracle Mobile Security Manager Server (`WLS_MSM1`)
   - Oracle Access Manager Policy Manager Server (`WLS_AMA1`)

   For example, to start Oracle Access Management Server on a Linux or UNIX system:

   ```
   DOMAIN_HOME/bin/startManagedWebLogic.sh WLS_OAM1
   ```

   On Windows systems:

   ```
   DOMAIN_HOME\bin\startManagedWebLogic.cmd WLS_OAM1
   ```

   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 Linux or UNIX systems:

```
DOMAIN_HOME/bin/startManagedWebLogic.sh WLS_OAM1 http://host:admin_server_port
```

On Windows systems:

```
DOMAIN_HOME\bin\startManagedWebLogic.cmd WLS_OAM1 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 Linux or UNIX systems:

```
DOMAIN_HOME/bin/startManagedWebLogic.sh WLS_OAM1 http://host:admin_server_port
-Dweblogic.management.username=user_name
-Dweblogic.management.password=password
-Dweblogic.system.StoreBootIdentity=true
```

On Windows systems:

```
DOMAIN_HOME\bin\startManagedWebLogic.cmd WLS_OAM1 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 Linux or UNIX systems:

```
DOMAIN_HOME/startManagedWebLogic_readme.txt
```

On Windows systems:

```
DOMAIN_HOME\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:

   ```
   DOMAIN_HOME/bin/stopManagedWebLogic.sh \
   {SERVER_NAME} {ADMIN_URL} {USER_NAME} {PASSWORD}
   ```

2. Stop the Oracle WebLogic Administration Server by executing the following command:

   ```
   DOMAIN_HOME/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

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 Linux or 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 Linux or 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 Linux or 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 Linux or 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.

E

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 E–1, leaving all other properties at their existing values.

Table E–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 E–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**.

      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.

F

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 (11.1.2.3.0).

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 might experience problems when you try to reinstall the software. Following the procedures in this appendix ensures that the software is properly removed.

F.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

F.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 Linux or 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 Linux or 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` (Linux or UNIX) or the *IAM_HOME*`\oui\bin directory` (Windows).
4. Invoke the Deinstaller from command line using the `-deinstall` option. For example:

   On Linux or 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.

F.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 Linux or 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 Linux or 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 Linux or 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.

F.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(11.1.2) 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.

G

Troubleshooting the Installation

This appendix describes solutions to common problems that you might encounter when installing Oracle Identity and Access Management.

It contains the following topics:

G.1 General Troubleshooting Tips

If you encounter an error during installation:

- Consult the Oracle Fusion Middleware 11*g* Release 2 (11.1.2.3.0) Release Notes. 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 F, "Deinstalling and Reinstalling Oracle Identity and Access Management" for more information.
  3. Correct the issue that caused the error.
  4. Restart the installation.

- If an error occurred while configuring Oracle Identity Manager using the Oracle Identity Manager Configuration Wizard:
  1. Note the error and review the configuration log files.
  2. Verify whether the dependencies are met. For example, Administration Server and Database should be up and running.
  3. Correct the issue that caused the error.
  4. Restart the Oracle Identity Manager Configuration Wizard.

G.2 Installation Log Files

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

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

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

The server log files are created in the *DOMAIN_HOME*/server/*servername*/logs directory.

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

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

G.3 Password for OAM Schema on Oracle Database 11*g* Expires Every 180 Days

The default password lifetime used for a user created on a newly installed Oracle Database 11*g* database is 180 days. After 180 days, the password automatically expires. When the Oracle Access Manager (OAM) schema password expires, the OAM environment will become inoperable.

To avoid this problem, you can do one of the following:

Solution 1: Change the default password policy for the database by configuring the password settings in the DEFAULT database profile (or in another relevant profile assigned to the OAM schema) so that the current OAM schema password will never expire.

To do this, you can use the ALTER PROFILE statement to set the PASSWORD_LIFE_TIME and PASSWORD_GRACE_TIME parameters to UNLIMITED in the OAM schema user's profile.

For more information about the password-related settings and how to configure them, see "Configuring Password Settings in the Default Profile" in the *Oracle Database Security Guide*.

See *Oracle Database SQL Language Reference* for more information about using `ALTER PROFILE` to modify the default password settings.

or

Solution 2: Reset the password before it expires.

To reset the OAM schema password on an Oracle Database 11*g* database, you must update the password for both the OPSS schema and OAM schema in the WebLogic Server Administration Console and then update the passwords in the database.

1. Update the password for OPSS in the WebLogic Server Administration Console:
    1. From the **Domain Structure** menu, expand **Services** and click **Data Sources**.
    2. Select the **opss-DBDS** data source in the Data Sources table.
    3. Select the **Configuration > Connection Pool** sub tab.
    4. Click **Lock & Edit** in the Change Center.
    5. Enter a new password for the OPSS schema in the **Password** and **Confirm Password** fields.
    6. Click **Save** to save the new password.
2. Update the password for OAM in the WebLogic Server Administration Console:
    1. From the **Domain Structure** menu, expand **Services** and click **Data Sources**.
    2. Select the **oamDS** data source in the Data Sources table.
    3. Select the **Configuration > Connection Pool** sub tab.
    4. Enter a new password for the OAM schema in the **Password** and **Confirm Password** fields.
    5. Click **Save** to save the new password, and then click **Activate Changes** in the Change Center.
3. Stop the servers in your environment.
4. Log on to sqlplus as the `SYS` database user, and update the schema passwords in the database:

    ```
    SQL> ALTER USER OAM_SCHEMA_USER IDENTIFIED BY NEW_PASSWORD;
    SQL> ALTER USER OPSS_SCHEMA_USER IDENTIFIED BY NEW_PASSWORD;
    ```

    For example:

    ```
    SQL> ALTER USER DEV_OAM IDENTIFIED BY password;
    SQL> ALTER USER DEV_OPSS IDENTIFIED BY password;
    ```

5. Start WLST from the *MW_HOME*`/oracle_common/common/bin` directory. For example:

    ```
    cd MW_HOME/oracle_common/common/bin
    ./wlst.sh
    ```

6. Run the WLST `modifyBootStrapCredential` command as follows:

    ```
    modifyBootStrapCredential(jpsConfigFile='DOMAIN_
    HOME/config/fmwconfig/jps-config.xml', username='prefix_OPSS', password='new_
    password')
    ```

7. Exit WLST:

    ```
    exit()
    ```

8. Start the servers in your environment.

G.4 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".

G.5 Resolving Issues When Starting the Administration Server

After completing your installation and domain configuration, you must start the Oracle WebLogic Administration Server to get your deployments up and running, as described in Appendix C.1, "Starting the Stack." The following scenarios describe error and warning messages you might encounter when trying to start the Administration Server and what to do to resolve these issues.

- Unsupported Configuration Store Version Detected After Configuring Oracle Access Management

G.5.1 Unsupported Configuration Store Version Detected After Configuring Oracle Access Management

Symptom: After configuring Oracle Access Management 11*g* Release 2 (11.1.2.3.0) in a WebLogic domain, you might encounter the following warning when starting the Administration Server:

```
<Warning><oracle.oam.config><BEA-000000><Unsupported configuration store version
detected. Required "11.1.2.3.0" but found "11.1.2.1.0".>
```

Cause: This warning message appears only when you start the Administration Server for the first time because the value of `ProductRelease` is not set to `11.1.2.3.0` in the `oam-config.xml` file:

```
<Setting Name="ProductRelease" Type="xsd:string">11.1.2.1.0</Setting>
```

The `oam-config.xml` file (located in the *`DOMAIN_HOME`*`/config/fmwconfig` directory) stores the system configuration data for Oracle Access Management. When you start the Administration Server for the first time, `ProductRelease` is set to `11.1.2.1.0`, and the server is started with the 11.1.2.1.0 version of the Oracle Access Management configuration.

Solution: Restart the WebLogic Administration Server, as described in Appendix C, "Starting or Stopping the Oracle Stack." Restarting the Administration Server automatically updates the value of `ProductRelease` to the correct version. Then, the warning will no longer appear.

You can open the *`DOMAIN_HOME`*`/config/fmwconfig/oam-config.xml` file to verify that the value of `ProductRelease` shows `11.1.2.3.0`:

```
<Setting Name="ProductRelease" Type="xsd:string">11.1.2.3.0</Setting>
```

For more information about the `oam-config.xml` file, see "About the oam-config.xml Configuration Data File" in the *Administrator's Guide for Oracle Access Management*.

G.6 Need More Help?

If you cannot solve a problem using the information in this appendix, look for additional information in My Oracle Support at

`http://support.oracle.com`.

If you cannot find a solution to your problem, open a service request.

H

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:

H.1 Overview

Database tables in the Oracle Adaptive Access Manager database are divided into the following categories:

- Static partition tables
- Transactional partition tables
- Non-partitioned tables

> **Note:** All the tables contain the composite partition (RANGE, HASH). The Range partition is created using `CREATE_TIME` while the `HASH` key is defined based on application logic.
>
> Table H–1 lists the Oracle Adaptive Access Manager partition tables. All the other tables are non-partitioned.

Table H–1 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

H.2 Partition Add Maintenance

After the initial Oracle Adaptive Access Manager repository setup, the following stored procedures are set up as dbms_jobs to maintain the partitions on a regular basis:

- Sp_Oaam_Add_Monthly_Partition
- Sp_Oaam_Add_Weekly_Partition

H.2.1 Sp_Oaam_Add_Monthly_Partition

This stored procedure adds partitions for tables with the monthly frequency.

The script runs at the end of each month to create partitions for the following month. To simultaneously add partitions for subsequent months, the partitions are added based on the partition of the previous month.

If this stored procedure fails to exceute (if your monthly partition is missing), you may see database errors, `"ORA-14400 and ORA-14401,"` forcing the Oracle Adaptive Access Manager application to stop.

H.2.2 Sp_Oaam_Add_Weekly_Partition

This stored procedure adds partitions for tables with the weekly frequency.

The script runs at the end of each week to create partitions for the following week. To simultaneously add partitions for subsequent weeks, the partitions are added based on the partition of the previous week.

If this stored procedure fails to exceute (if your weekly partition is missing), you may see database errors, "ORA-14400 and ORA-14401," forcing the Oracle Adaptive Access Manager application to stop.

H.3 Partition Maintenance Scripts

After the initial Oracle Adaptive Access Manager repository setup, use the following scripts with purging or archiving maintenance scripts to maintain the partitions on a regular basis:

- drop_monthly_partition_tables.sql
- drop_weekly_partition_tables.sql
- add_monthly_partition_tables.sql
- add_weekly_partition_tables.sql

The above mentioned scripts are located 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.

H.3.1 drop_monthly_partition_tables.sql

You can use this script to drop partitions for tables with the monthly frequency. You should run this script at the end of each month to drop partitions older than sixth months, based on the requirements of the Oracle Adaptive Access Manager application. Note that these tables will have six partitions at a given time.

H.3.2 drop_weekly_partition_tables.sql

You can use this script to drop partitions for tables with the weekly frequency. You should run this script either at the end of every fourteenth day or at the end of third week from the day the Oracle database was created to the dropping of partitions older than two weeks, based on the requirements of the Oracle Adaptive Access Manager application.

H.3.3 add_monthly_partition_tables.sql

You can use this script to add partitions for tables with the monthly frequency. You should run this script at the end of each month to create partitions for the following month. To add partitions for subsequent months at the same time, run this script multiple times. When you run the script multiple times, partitions are added based on the previous month's partition.

H.3.4 add_weekly_partition_tables.sql

You can use this script to add partitions for tables with the weekly frequency. You should run this script at the end of each month to create partitions for the following week. To add partitions for subsequent weeks at the same time, run this script multiple times. When you run the script multiple times, partitions are added based on the previous week's partition.

Software Deinstallation Screens

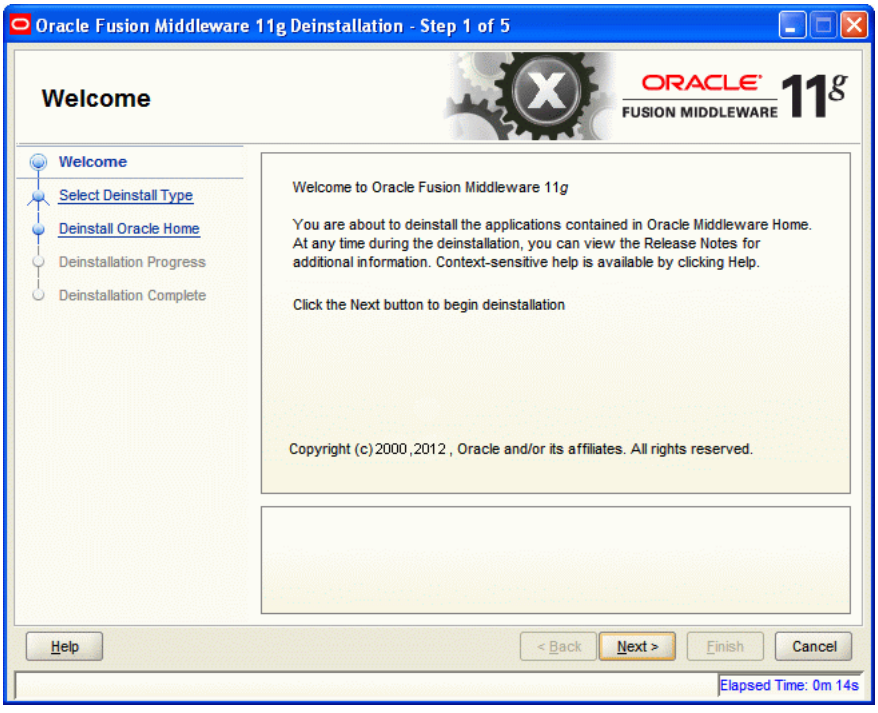
This appendix describes the screens of the Oracle Fusion Middleware 11*g* Deinstallation Wizard that enables you to remove the Oracle Identity and Access Management software from your machine.

This appendix contains the following topics:

I.1 Welcome

The Welcome screen is the first screen that appears when you start the Oracle Fusion Middleware 11*g* Deinstallation Wizard.

Figure I–1 Welcome Screen



Click **Next** to continue.

I.2 Select Deinstallation Type

Select the type of deinstallation you want to perform.

Figure I–2 Select Deinstallation Type Screen

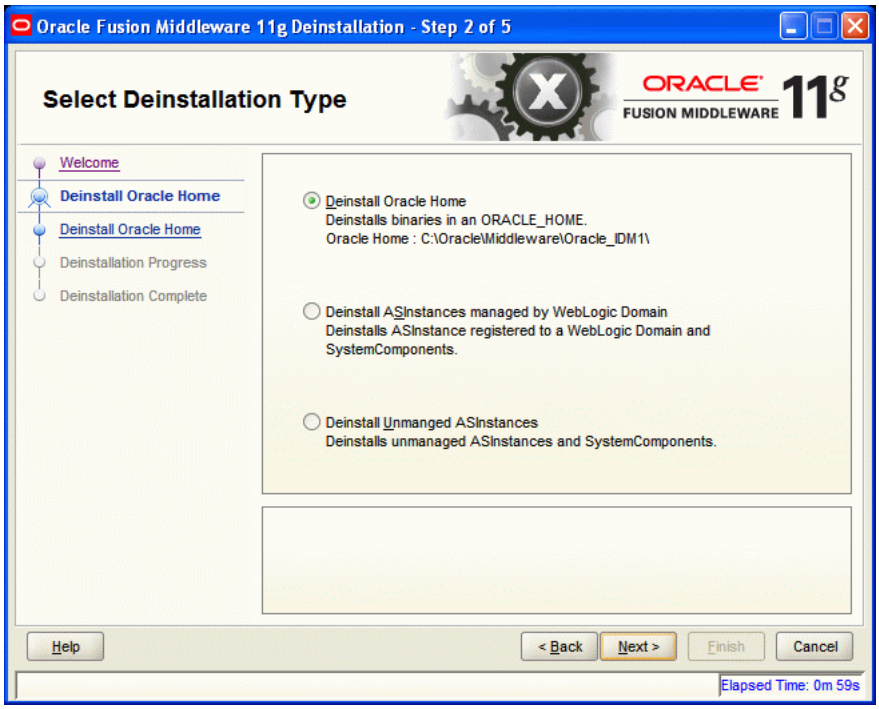


Table I–1 Deinstallation Types

Type	Description
Deinstall Oracle Home	Select this option to deinstall the binaries contained in the listed Oracle Identity 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.

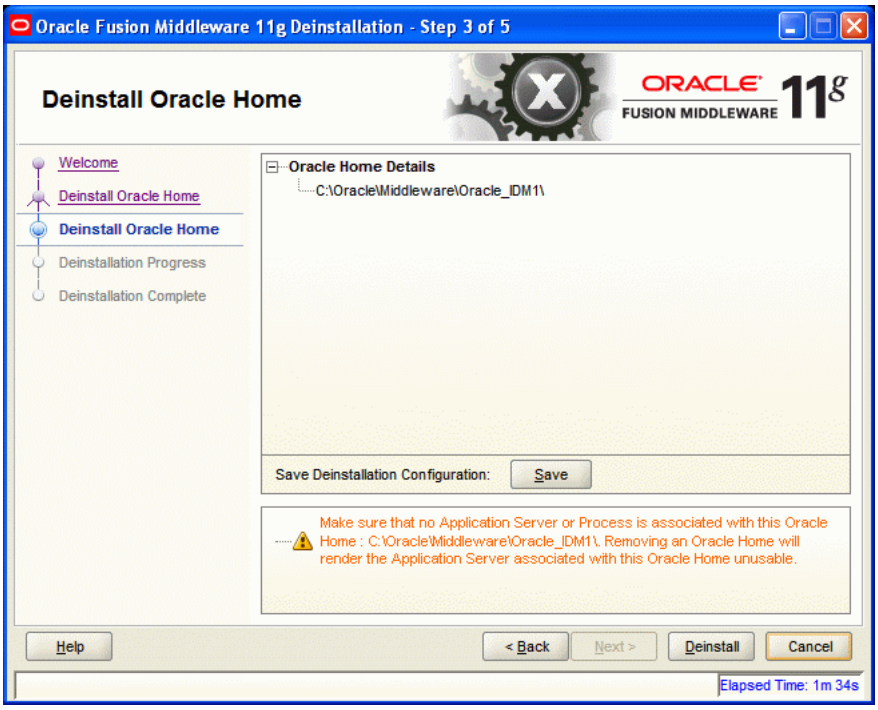
I.2.1 Option 1: Deinstall Oracle Home

If you selected **Deinstall Oracle Home** on the Select Deinstallation Type screen, the following screen appears:

I.2.1.1 Deinstall Oracle Home

This screen shows the Oracle Home directory that is about to be deinstalled. It is the Oracle Home directory in which the deinstaller was started.

Figure I–3 Deinstall Oracle Home Screen



Verify that this is the correct directory, and also verify that there are no processes associated with this Oracle Home.

Click **Deinstall** to start the deinstallation process.

I.2.2 Option 2: Deinstall ASInstances managed by WebLogic Domain

If you selected **Deinstall ASInstances managed by WebLogic Domain** on the Select Deinstallation Type screen, the following screens appears:

- Specify WebLogic Domain Detail
- Select Managed Instance
- Deinstallation Summary (Managed Instance)

I.2.2.1 Specify WebLogic Domain Detail

Specify the WebLogic Domain credentials:

- **Domain Host Name**

  The name of the system on which the WebLogic Domain is running.

- **Domain Port No**

  Listen port number of the domain. The default port number is `7001`.

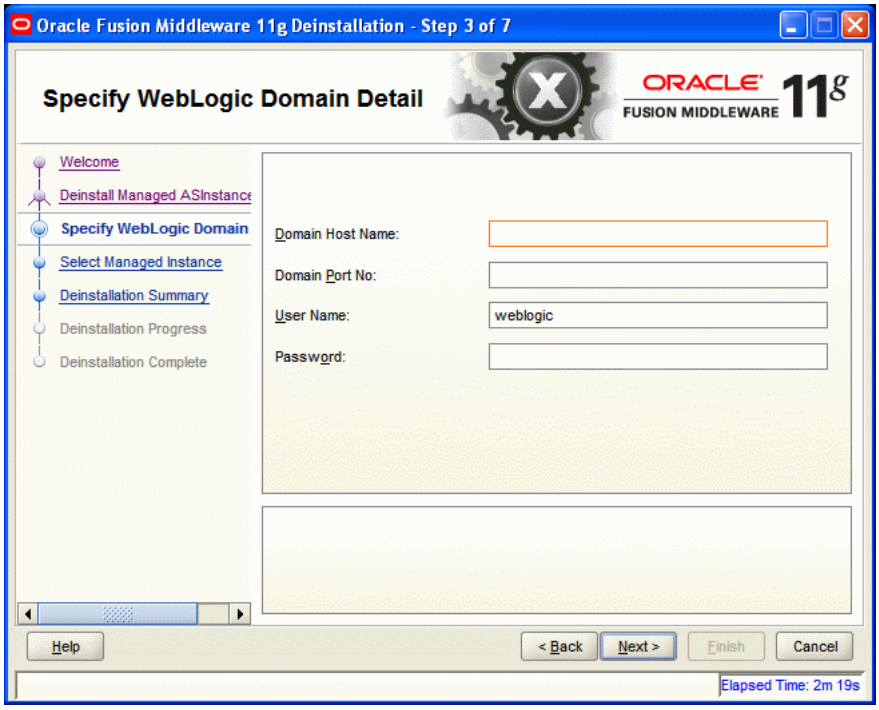
- **User Name**

  The WebLogic Domain user name.

- **Password**

  The password of the WebLogic Domain user.

Figure I–4 Specify WebLogic Domain Detail Screen

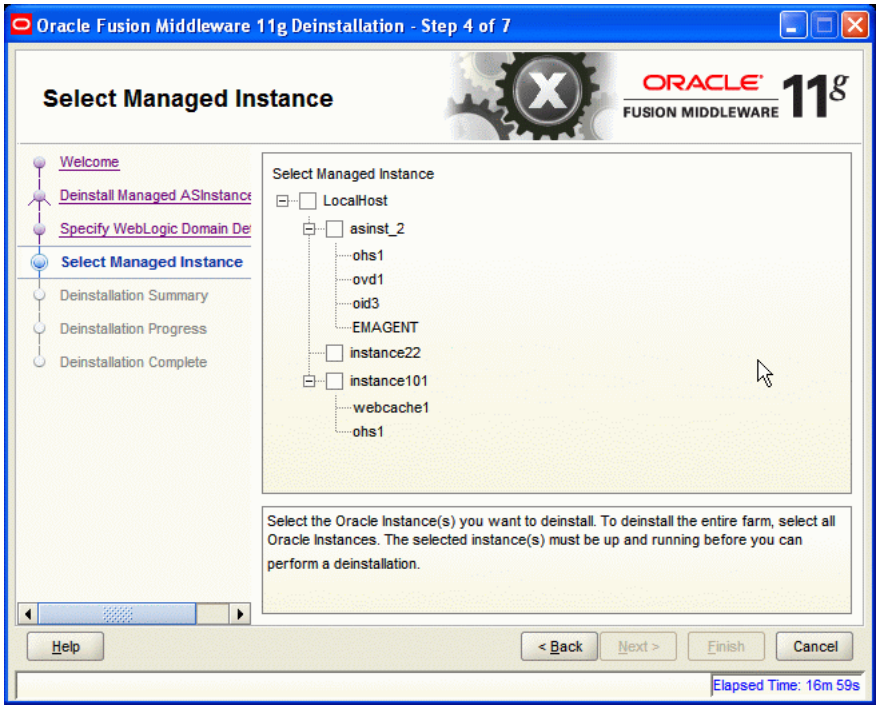


Click **Next** to continue.

I.2.2.2 Select Managed Instance

Select the managed instance you want to deinstall.

Figure I–5 Select Managed Instance Screen

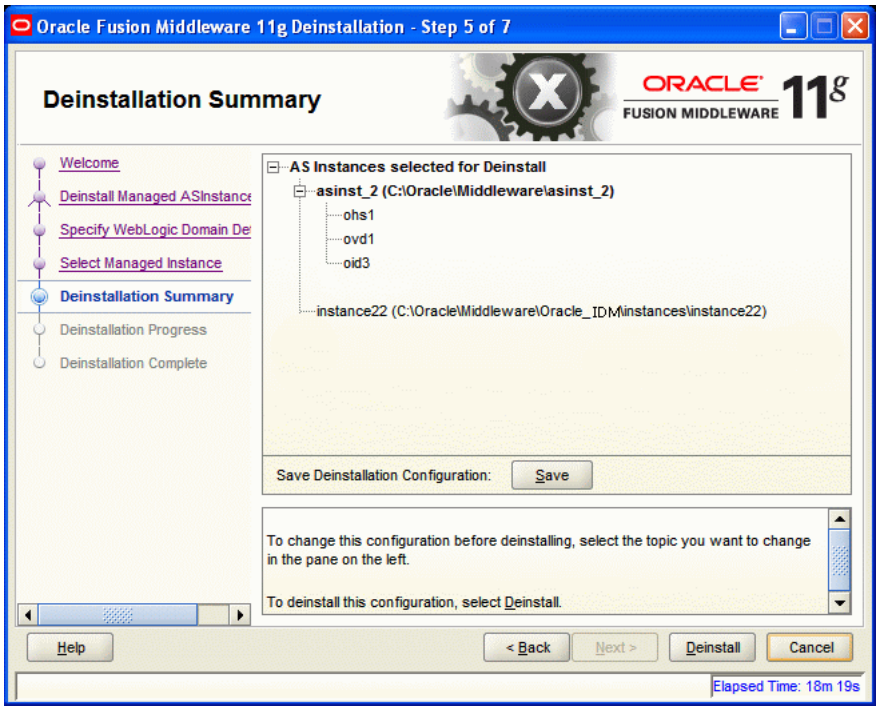


Click **Next** to continue.

I.2.2.3 Deinstallation Summary (Managed Instance)

Verify that the specified instance is the one you want to deinstall.

Figure I–6 Deinstallation Summary Screen



Click **Deinstall** to start the deinstallation process.

I.2.3 Option 3: Deinstall Unmanaged ASInstances

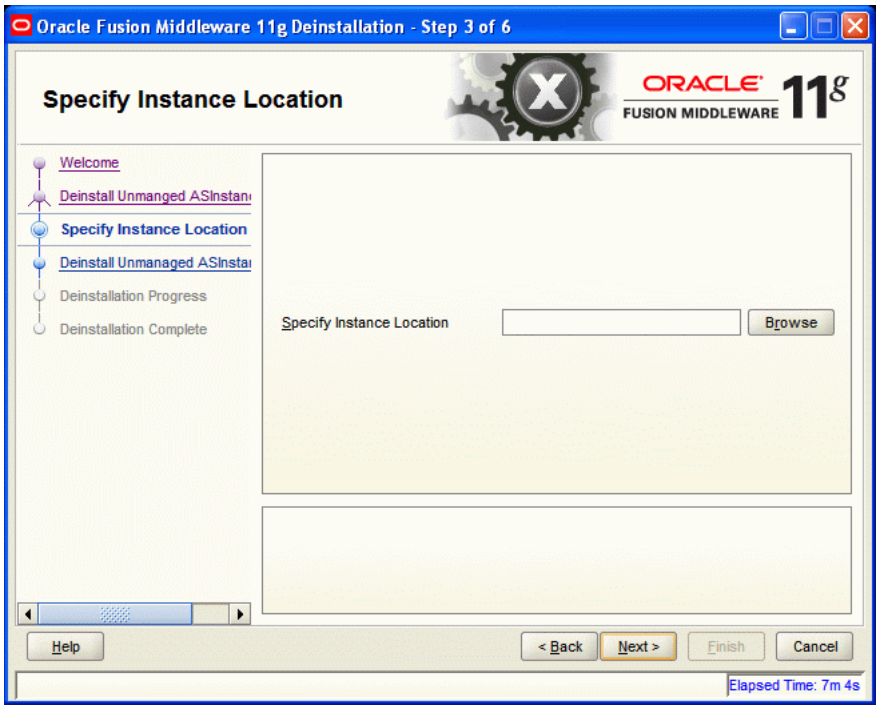
If you selected **Deinstall Unmanaged ASInstances** on the Select Deinstallation Type screen, the following screen appears:

- Specify Instance Location
- Deinstallation Summary (Unmanaged ASInstance)

I.2.3.1 Specify Instance Location

Specify the full path to your Oracle Instance directory. If you are unsure, click **Browse** to find this directory on your system.

Figure I–7 Specify Instance Location Screen

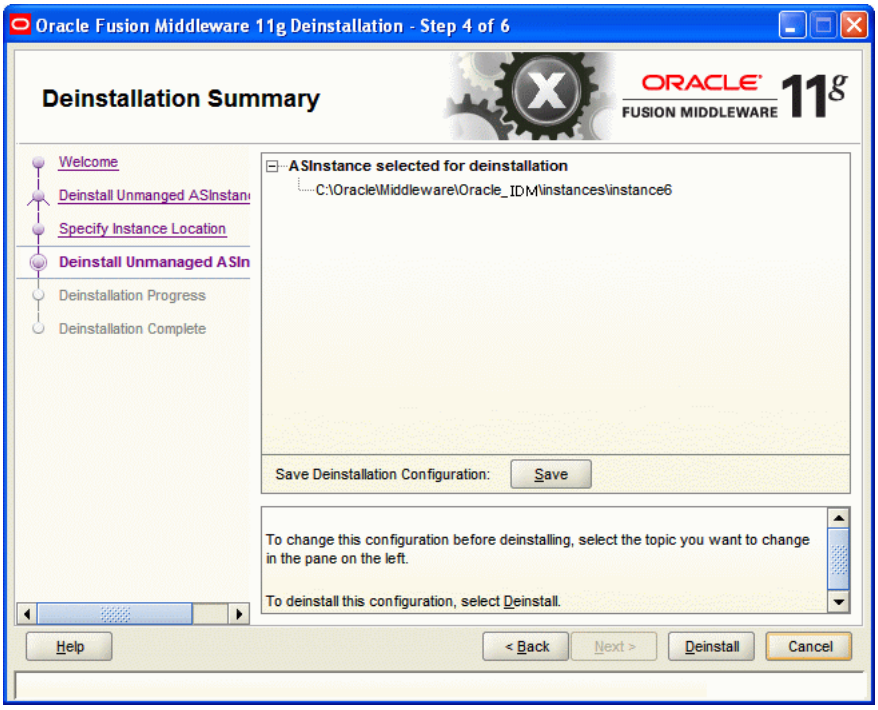


Click **Next** to continue.

I.2.3.2 Deinstallation Summary (Unmanaged ASInstance)

Verify that the specified instance is the one you want to deinstall.

Figure I–8 Deinstallation Summary Screen

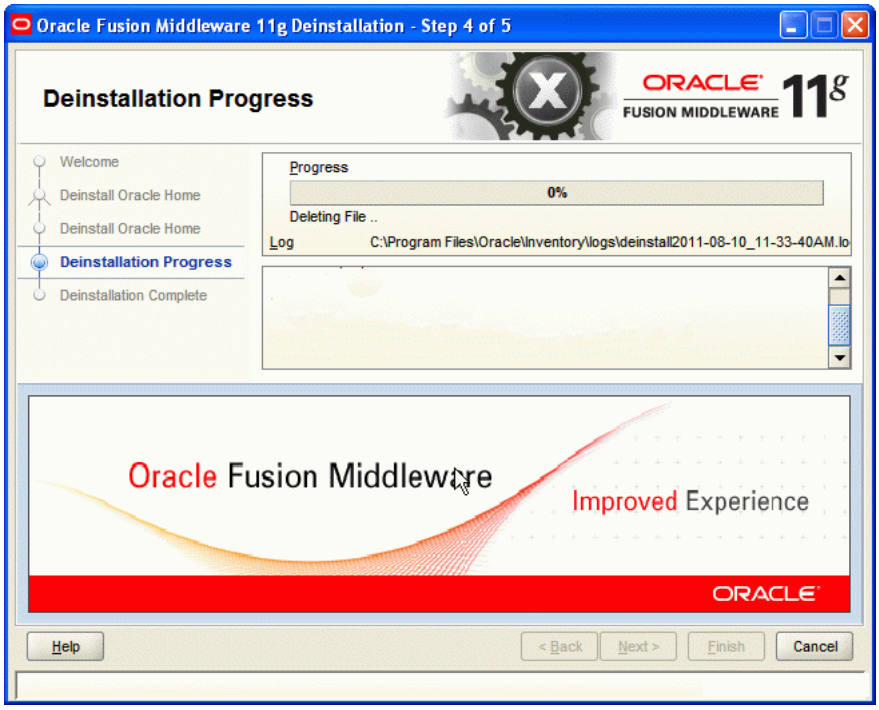


Click **Deinstall** to start the deinstallation process.

I.3 Deinstallation Progress

This screen shows you the progress of the deinstallation.

Figure I–9 Deinstallation Progress Screen



If you want to quit before the deinstallation is completed, click **Cancel**.

I.4 Deinstallation Complete

This screen summarizes the deinstallation that was just completed.

Figure I–10 Deinstallation Complete Screen

Click **Finish** to dismiss the deinstaller.