Oracle® Fusion Middleware

Quick Installation Guide for Oracle Identity and Access Management

11*g* Release 2 (11.1.2)

E27794-02

August 2012

ORACLE®

Oracle Fusion Middleware Quick Installation Guide for Oracle Identity and Access Management, 11*g* Release 2 (11.1.2)

E27794-02

Primary Author: Nisha Singh

Contributing Author: Rekha Kamath, Ashish Daniel Thomas

Contents

Preface

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

Audience

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

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

Documentation Accessibility

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

Access to Oracle Support

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

Related Documents

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

`http:/docs.oracle.com/`

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

Oracle Fusion Middleware

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

High Availability

- *Oracle Fusion Middleware High Availability Guide*

Oracle Fusion Middleware Repository Creation Utility

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

Oracle Identity Manager

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

Oracle Access Management

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

Oracle Adaptive Access Manager

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

Oracle Identity Navigator

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

Conventions

The following text conventions are used in this document:

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

1

Understanding Oracle Identity and Access Management Installation

This chapter provides an overview of Oracle Identity and Access Management 11*g* Release 2 (11.1.2) installation.

It describes the following topics:

- Section 1.1, "Overview of Oracle Identity and Access Management 11g Release 2 (11.1.2) Installation"
- Section 1.2, "Additional Information for Deploying 11g Release 2 (11.1.2)"
- Section 1.3, "Silent Installation of Oracle Identity and Access Management 11g Release 2 (11.1.2)"

1.1 Overview of Oracle Identity and Access Management 11*g* Release 2 (11.1.2) Installation

Oracle Identity and Access Management 11*g* Release 2 (11.1.2) includes the following components:

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

Note: The steps for installing Oracle Unified Directory 11*g* Release 2 are not covered in this guide.

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

1.2 Additional Information for Deploying 11*g* Release 2 (11.1.2)

This section describes additional sources for 11*g* Release 2 (11.1.2) deployment, including documentation on the following subjects:

- Upgrading to Oracle Identity and Access Management 11g Release 2 (11.1.2)
- Installing Oracle Identity and Access Management 11g Release 2 (11.1.2) for High Availability
- Deploying Oracle Unified Directory with Oracle Identity and Access Management 11g Release 2 (11.1.2)

Note: For a list of documents that provide additional information about Oracle Identity and Access Management components, see the "Related Documents" section in the preface of this guide.

1.2.1 Upgrading to Oracle Identity and Access Management 11*g* Release 2 (11.1.2)

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). To upgrade an Oracle Identity and Access Management component, refer to *Oracle Fusion Middleware Upgrade and Migration Guide for Oracle Identity and Access Management*.

1.2.2 Installing Oracle Identity and Access Management 11*g* Release 2 (11.1.2) for High Availability

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

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

1.2.3 Deploying Oracle Unified Directory with Oracle Identity and Access Management 11*g* Release 2 (11.1.2)

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

- Oracle Unified Directory 11*g* Release 2 in an Oracle Identity and Access Management 11*g* Release 2 (11.1.2) domain.
- Oracle Identity and Access Management 11*g* Release 2 (11.1.2) products in an Oracle Unified Directory 11*g* Release 2 domain.

Note:

- ❏ This guide does not cover the steps to install Oracle Unified Directory 11*g* Release 2.
- ❏ For information about installing Oracle Unified Directory 11*g* Release 2, see the *Oracle Unified Directory Installation Guide*.

1.3 Silent Installation of Oracle Identity and Access Management 11*g* Release 2 (11.1.2)

To perform a silent installation of Oracle Identity and Access Management 11*g* Release 2 (11.1.2), see Appendix H.4 "Performing a Silent Installation" in *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

2

Preparing to Install Oracle Identity and Access Management

This chapter provides information that you should review before installing Oracle Identity and Access Management 11*g* Release 2 (11.1.2) components.

It describes the following topics:

2.1 Reviewing System Requirements and Certification

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

- *Oracle Fusion Middleware System Requirements and Specifications*

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

- *Oracle Fusion Middleware Supported System Configurations*

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

- For interoperability and compatibility issues that may arise when installing Oracle Identity and Access Management 11*g* Release 2 (11.1.2), refer to *Oracle Fusion Middleware Interoperability and Compatibility Guide for Oracle Identity and Access Management*.

  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 the `access-bridge.jar` file and the `jaccess-1_4.jar` file your installation location to the `jre\lib\ext` directory.
4. Copy the `WindowsAccessBridge.dll`, `JavaAccessBridge.dll`, and the `JAWTAccessBridge.dll` file 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 that you must identify in most of the Oracle Identity and Access Management installations and configurations.

The following are the common directories described in this section:

- 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 that you are installing, under the Oracle Middleware Home that you identify in this field. The Oracle Middleware Home directory is commonly referred to as *`MW_HOME`*.

2.3.2 Oracle Home Directory

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

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

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 that you enter in the Oracle Middleware Home Location field.

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

2.3.4 Oracle WebLogic Domain Directory

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

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

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

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

2.3.5 WebLogic Server Directory

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

2.4 Determining Port Numbers

If you want to install an Oracle Identity and Access Management 11g Release 2 (11.1.2) component against an existing Oracle Identity and Access Management 11g Release 2 (11.1.2) component, you may need to identify the ports for the existing component. For example, if you want to install Oracle Identity Manager 11g Release 2 (11.1.2) against an existing Oracle Internet Directory 11g Release 2 (11.1.2) component, you must identify its port when you install Oracle Identity Manager.

2.5 Locating Installation Log Files

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

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

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

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

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

3

Installing and Configuring Oracle Identity and Access Management (11.1.2)

This chapter describes the following topics:

- Section 3.1, "Overview of Oracle Identity and Access Management (11.1.2) Installation"
- Section 3.2, "Installing and Configuring Oracle Identity and Access Management (11.1.2)"

3.1 Overview of Oracle Identity and Access Management (11.1.2) Installation

Table 3–1 lists the general installation and configuration tasks that apply to Oracle Identity and Access Management 11*g* Release 2 (11.1.2.0.0) products.

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

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

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

No.	Task	Description
7	For Oracle Identity Manager users only: Install the latest version of Oracle SOA Suite 11*g* (11.1.1.6.0).	For more information, see Section 3.2.5, "Installing Oracle SOA Suite 11.1.1.6.0 (Oracle Identity Manager Users Only)".
8	Start the Oracle Identity and Access Management installer.	For more information, see Section 3.2.6, "Starting the Oracle Identity and Access Management Installer".
9	Install the Oracle Identity and Access Management 11*g* software.	For more information, see Section 3.2.7, "Installing Oracle Identity and Access Management (11.1.2)".
10	Run the Oracle Fusion Middleware Configuration Wizard to configure your Oracle Identity and Access Management products in a new or existing WebLogic domain.	**Note:** If you are using Oracle Identity Manager, you must perform additional configuration after configuring Oracle Identity Manager in a WebLogic domain. For more information, see "Configuring Oracle Identity Management" in *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.
11	Configure the Database Security Store.	For more information, see Section 3.2.9, "Configuring Database Security Store for an Oracle Identity and Access Management Domain".
12	Start the servers.	You must start the Administration Server and all Managed Servers for the components that you have configured. For more information, see Section B.1, "Starting the Stack".

3.2 Installing and Configuring Oracle Identity and Access Management (11.1.2)

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

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

- Obtaining the Oracle Fusion Middleware Software
- Reviewing the Database Requirements
- Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU)
- Reviewing the WebLogic Server and Middleware Home Requirements
- Installing Oracle SOA Suite 11.1.1.6.0 (Oracle Identity Manager Users Only)
- Starting the Oracle Identity and Access Management Installer
- Installing Oracle Identity and Access Management (11.1.2)
- Configuring Oracle Identity and Access Management (11.1.2) Products
- Configuring Database Security Store for an Oracle Identity and Access Management Domain
- Starting the Servers

3.2.1 Obtaining the Oracle Fusion Middleware Software

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

- Oracle WebLogic Server 11*g* Release 1 (10.3.6)
- Oracle Database
- Oracle Repository Creation Utility
- Oracle Identity and Access Management Suite
- Oracle SOA Suite 11.1.1.6.0 (required for Oracle Identity Manager only)

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

3.2.2 Reviewing the Database Requirements

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

The following database versions are supported:

- 10.2.0.4 and higher
- 11.1.0.7 and higher
- 11.2.0.1 and higher

Note: For information about RCU requirements for Oracle Databases, see "RCU Requirements for Oracle Databases" in the *Oracle Fusion Middleware System Requirements and Specifications* document.

3.2.2.1 Oracle Database 11.1.0.7 Patch Requirements for Oracle Identity Manager

To identify the patches required for Oracle Identity Manager 11.1.2 configurations that use Oracle Database 11.1.0.7, refer to the Oracle Identity Manager section of the 11*g* Release 2 *Oracle Fusion Middleware Release Notes*.

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

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

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

- Oracle Identity Navigator

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

> **Note:** RCU is available only on Linux and Windows platforms. Use the Linux RCU to create schemas on supported UNIX databases. Use the Windows RCU to create schemas on supported Windows databases. After you extract the contents of the `rcuHome.zip` file to a directory, you can see the executable file `rcu` in the `BIN` directory.
>
> For information on launching and running RCU, see the "Launching RCU with a Variety of Methods" and "Running Oracle Fusion Middleware Repository Creation Utility (RCU)" topics in *Oracle Fusion Middleware Repository Creation Utility User's Guide*. For information about troubleshooting RCU, see "Troubleshooting Repository Creation Utility"in *Oracle Fusion Middleware Repository Creation Utility User's Guide*.

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

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

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

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

> **Note:** For information about Oracle Adaptive Access Manager schema partitions, see *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

- For Oracle Access Management, select the **Identity Management - Oracle Access Manager** schema. When you select the **Identity Management - Oracle Access Manager** schema, the following schemas are also selected, by default:

  > **Note:** If you want to use Transparent Data Encryption (TDE) for Oracle Access Management, you must set up TDE for Oracle Access Management before creating the Oracle Access Management schema. For more information, see "Optional: Setting Up TDE for Oracle Access Management" in *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

  - AS Common Schemas - Oracle Platform Security Services
  - AS Common Schemas - Metadata Services
  - AS Common Schemas - Audit Services
- For Oracle Entitlements Server, select the **Identity Management - Oracle Entitlements Server** schema. When you select the Identity Management - Oracle Entitlements Server schema, the following schemas are also selected, by default:
  - AS Common Schemas - Oracle Platform Security Services
  - AS Common Schemas - Metadata Services
- For Oracle Privileged Account Manager, select the **Identity Management - Oracle Privileged Account Manager** schema. When you select the **Identity Management - Oracle Privileged Account Manager** schema, the following schemas are also selected, by default:
  - AS Common Schemas - Oracle Platform Security Services
  - AS Common Schemas - Metadata Services
- For Oracle Identity Navigator, select the **AS Common Schemas - Oracle Platform Security Services** schema. By default, the **AS Common Schemas - Metadata Services** schema is also selected.

  > **Note:** When you create a schema, ensure that you note down the 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.

For more information about creating schemas using the RCU, see *Oracle Fusion Middleware Repository Creation Utility User's Guide*.

3.2.4 Reviewing the WebLogic Server and Middleware Home Requirements

Before you install Oracle Identity and Access Management 11*g* Release 2 (11.1.2) components, ensure that you have installed Oracle WebLogic Server and created a Middleware Home directory.

> **Note:** When you install Oracle WebLogic Server on a 64-bit platform, using the generic jar file, JDK is not installed with Oracle WebLogic Server. You must install JDK separately, before installing Oracle WebLogic Server.
>
> Ensure that the JDK version you select is Java SE 6 Update 24 or higher.

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

For information about installing the Oracle WebLogic Server, see "Preparing for Installation" and "Running the Installation Program in Graphical Mode" in *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*.

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

3.2.5 Installing Oracle SOA Suite 11.1.1.6.0 (Oracle Identity Manager Users Only)

If you are installing Oracle Identity Manager, you must install Oracle SOA Suite 11.1.1.6.0. Note that only Oracle Identity Manager requires Oracle SOA Suite. This step is required because Oracle Identity Manager uses process workflows in Oracle SOA Suite to manage request approvals.

For more information about installing Oracle SOA Suite 11.1.1.6.0, see *Oracle Fusion Middleware Installation Guide for Oracle SOA Suite and Oracle Business Process Management Suite*.

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

3.2.6 Starting the Oracle Identity and Access Management Installer

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

Notes:

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

Start the installer by executing one of the following commands:

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

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

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

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

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

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

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

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

3.2.7 Installing Oracle Identity and Access Management (11.1.2)

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

It includes the following sections:

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

3.2.7.1 Products Installed

Performing the installation in this section installs the following products:

- Oracle Identity Manager
- Oracle Access Management

  Note: Oracle Identity and Access Management 11g Release 2 (11.1.2) contains Oracle Access Management which includes the following service providers:

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

  For more information about these service providers, see "Oracle Product Introduction" in *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.

- Oracle Adaptive Access Manager

  Note: For Oracle Identity and Access Management 11.1.2, Oracle Adaptive Access Manager includes the following components:

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

- Oracle Identity Navigator
- Oracle Entitlements Server

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

  To install and configure Oracle Entitlements Server Client, see Section 8.6, "Installing Oracle Entitlements Server Client" in *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

- Oracle Privileged Account Manager

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

- Oracle Access Management Mobile and Social

Notes:

- For an introduction to the Oracle Access Management Mobile and Social, see "Understanding Mobile and Social" chapter in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.
- Oracle Access Management Mobile and Social standalone template does not use the database security store. If Oracle Access Management Mobile and Social is deployed standalone in a domain, and if you want to extend that domain to include other Oracle Identity and Access Management 11*g*R2 components, you must complete the following additional steps:

  1. Create an **Oracle Platform Security Services** schema using the Oracle Fusion Middleware Repository Creation Utility (RCU). For more information, see Section 3.2.3, "Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU)".
  2. Extend the Oracle Access Management Mobile and Social domain with **Oracle Platform Security Service 11.1.1.0 [IAM_Home]** template.

     For information on extending WebLogic Server domains, see "Extending WebLogic Domains" chapter in the *Oracle Fusion Middleware Creating Domains Using the Configuration Wizard* guide.

  The Oracle Access Management Mobile and Social domain can now be extended to include other Oracle Identity and Access Management 11*g* R2 components.

3.2.7.2 Dependencies

The installation in this section depends on the following:

- Oracle WebLogic Server 11*g* Release 1 (10.3.6) or Oracle WebLogic Server 11*g* Release 1 (10.3.5)
- Oracle Database and any required patches
- Oracle SOA Suite 11.1.1.6.0 (required for Oracle Identity Manager only)
- JDK (Java SE 6 Update 24 or higher) or JRockit

3.2.7.3 Procedure

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

1. Start your installation by performing all of the steps listed in Section 3.2.6, "Starting the Oracle Identity and Access Management Installer". After you complete those steps, the Welcome screen appears.
2. Click **Next** to proceed. The Install Software Updates screen appears. Select whether or not you want to search for updates and click **Next**.
3. The Prerequisite Checks screen appears. If all prerequisite checks pass inspection, click **Next**. The Specify Installation Location screen appears.
4. On the Specify Installation Location screen, enter the path to the Oracle Middleware Home that was created when you installed Oracle WebLogic Server 11*g* Release 1 (10.3.6) or Oracle WebLogic Server 11*g* Release 1 (10.3.5) on your system. Ensure that Oracle WebLogic Server is already installed on the system in the same Middleware Home. This directory is the same as the Oracle Home created in the Oracle WebLogic Server installation.

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

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

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

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

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

   By default the installer chooses an alternate name `Oracle_IDM2` if `Oracle_IDM1` oracle home exists and has Oracle Identity Management components installed. This should not be changed to `Oracle_IDM1`.

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

left navigation page and modify your choices. To continue installing Oracle Identity and Access Management, click **Install**. The Installation Progress screen appears. Click **Next**.

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

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

---

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

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

   After installing the Oracle Identity and Access Management software, you must proceed to Section 3.2.8, "Configuring Oracle Identity and Access Management (11.1.2) Products," to configure Oracle Identity and Access Management products in a new or existing WebLogic domain.

3.2.7.4 Understanding the Directory Structure After Installation

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

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

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

3.2.8 Configuring Oracle Identity and Access Management (11.1.2) 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 component, you can choose one of the following configuration options:

- Create a New Domain
- Extend an Existing Domain

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

Create a New Domain

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

Extend an Existing Domain

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

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

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

- "Configuring Oracle Identity Navigator" in *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*
- "Configuring Oracle Access Management" in *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*
- "Configuring Oracle Adaptive Access Manager" in *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*
- "Installing and Configuring Oracle Entitlements Server" in *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*
- "Configuring Oracle Privileged Account Manager" in *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*
- "Configuring Oracle Access Management Mobile and Social" in *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*

If you are configuring Oracle Identity Manager, you must run the Oracle Identity Manager Configuration Wizard after configuring a domain, to configure Oracle Identity Manager Server, Oracle Identity Manager Design Console, and Oracle Identity Manager Remote Manager as described in "Starting the Oracle Identity Manager 11*g* Configuration Wizard" in *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*. For more information, see the following sections:

- "Configuring Oracle Identity Manager Server" in *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*
- "Optional: Configuring Oracle Identity Manager Design Console" in *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*
- "Optional: Configuring Oracle Identity Manager Remote Manager" in *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*

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

This section discusses the following topics:

- Before Configuring Database Security Store

- Configuring the Database Security Store

3.2.9.1 Overview

You must run the `configureSecurityStore.py` script to configure the Database Security Store as it is the only security store type supported by the Oracle Identity & Access Management 11*g* Release 2 (11.1.2).

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

For example:

On Windows:

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

On UNIX:

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

Table 3–2 describes the parameters you that you may specify on the command line.

Table 3–2 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`.
`-p` *`password`*	The OPSS schema password.
`-k` *`keyfilepath`*	The directory containing the encryption key file `ewallet.p12`. If `-m join` is specified, this option is mandatory.
`-w` *`keyfilepassword`*	The password used when the domain's key file was generated. If `-m join` is specified, this option is mandatory.
`-u` *`username`*	The user name of the OPSS schema. If `-m fixjse` is specified, this option is mandatory.

3.2.9.2 Before Configuring Database Security Store

Each Oracle Identity and Access Management 11*g* Release 2 (11.1.2) domain must be configured to have a Database Security Store. Before you configure the Database Security Store for an Oracle Identity and Access Management 11g Release 2 (11.1.2) domain, you must identify the products to be configured in a single-domain scenario or in a multiple-domain scenario.

> **Note:** Irrespective of the number of domains in a logical Oracle Identity and Access Management 11*g* Release 2 (11.1.2) deployment (a logical deployment is a collection of Oracle Identity and Access Management products running in one or more domains and using a single database to hold product schemas), all domains share the same Database Security Store and use the same domain encryption key.
>
> The Database Security Store is **created** at the time of creating the first domain, and then each new domain created is **joined** with the Database Security Store already created.

3.2.9.3 Configuring the Database Security Store

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

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

Configuring the Database Security Store Using Create Option

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

On Windows:

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

For example:

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

On UNIX:

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

For example:

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

Configuring the Database Security Store Using the Join Option

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

the database security store, and then run the `configureSecurityStore.py` script as follows:

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

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

where:

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

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

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

On Windows:

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

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

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

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

For example:

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

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

On UNIX:

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

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

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

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

For example:

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

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

Validating the Database Security Store Configuration

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

On Windows:

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

For example:

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

On UNIX:

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

For example:

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

3.2.9.4 Example Scenarios for Configuring the Database Security Store

Consider the following example scenarios:

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

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

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

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

To achieve this, you must complete the following tasks:

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

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

   On Windows:

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

   On UNIX:

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

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

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

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

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

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

  To achieve this, you must complete the following tasks:

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

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

On Windows:

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

On UNIX:

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

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

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

   On Windows:

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

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

   On UNIX:

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

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

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

  To achieve this, extend the Oracle Access Manager 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 Manager domain (*oam_dom*), and they both share the same Database Security Store used by the Oracle Access Manager domain.

3.2.10 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 B.1, "Starting the Stack".

Deinstalling and Reinstalling Oracle Identity and Access Management

This appendix provides information about deinstalling and reinstalling Oracle Identity and Access Management 11g Release 2 (11.1.2). It contains the following topics:

- Section A.1, "Deinstalling Oracle Identity and Access Management"
- Section A.2, "Reinstalling Oracle Identity and Access Management"

> **Note:** Always use the instructions provided in this appendix for removing the software. If you try to remove the software manually, you may experience problems when you try to reinstall the software. Following the procedure in this appendix ensures that the software is properly removed.

A.1 Deinstalling Oracle Identity and Access Management

This section contains procedures for deinstalling Oracle Identity and Access Management. It describes the following topics:

- Deinstalling the Oracle Identity and Access Management Oracle Home
- Deinstalling the Oracle Common Home

A.1.1 Deinstalling the Oracle Identity and Access Management Oracle Home

The deinstaller attempts to remove the Oracle Home directory from which it was started. Before you choose to remove your Oracle Identity and Access Management Oracle Home directory, make sure that it is not in use by an existing domain, and that you stop all running processes that use this Oracle Home.

Deinstalling Oracle Identity and Access Management will not remove any WebLogic domains that you have created—it only removes the software in the Oracle Identity and Access Management Oracle Home directory.

> **Note:** The oraInventory is required for removing instances and Oracle Home. For example, on UNIX, it can be found in the following location:
>
> `/etc/oraInst.loc`

This section describes how to deinstall your Oracle Identity and Access Management Oracle Home using the graphical, screen-based deinstaller. However, you can also perform a silent deinstallation using a response file. A deinstall response file template that you can customize for your deinstallation is included in the `Disk1/stage/Response` directory on UNIX, or in the `Disk1\stage\Response` directory on Windows.

Perform the following steps to deinstall your Oracle Identity and Access Management Oracle Home using the graphical, screen-based deinstaller:

1. Verify your Oracle Identity and Access Management Oracle Home is not in use by an existing domain.
2. Stop all processes that use the Oracle Identity and Access Management Oracle Home.
3. Open a command prompt, and go to the *IAM_ORACLE_HOME*/oui/bin directory (UNIX) or the *IAM_HOME*\oui\bin directory (Windows) by running the following command:

   For UNIX:

   ```
   $ cd IAM_ORACLE_HOME/oui/bin directory
   ```

   For Windows:

   ```
   $ cd IAM_HOME\oui\bin directory
   ```

4. Invoke the Deinstaller from command line using the -deinstall option. For example:

   On UNIX:

   ```
   ./runInstaller -deinstall
   ```

   On Windows:

   ```
   setup.exe -deinstall
   ```

   The Welcome screen appears.
5. Click **Next**. The Deinstall Oracle Home screen appears.
6. 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.
7. Click **Finish** after the deinstallation progresses to 100%. The Deinstallation Complete screen appears.
8. Click **Finish** on the Deinstallation Complete screen to exit the deinstaller.

A.1.2 Deinstalling the Oracle Common Home

The *ORACLE_COMMON_HOME* directory located in the *MW_HOME* directory contains the binary and library files required for Oracle Enterprise Manager Fusion Middleware Control and Oracle Java Required Files (JRF). Before you deinstall the *ORACLE_COMMON_HOME* directory, ensure that no other Oracle Fusion Middleware software, such as Oracle SOA Suite, depends on *ORACLE_COMMON_HOME*. You cannot deinstall the *ORACLE_COMMON_HOME* directory until all software that depends on it has been deinstalled.

Perform the following steps to deinstall the *ORACLE_COMMON_HOME* directory:

1. Stop all processes that use the *ORACLE_COMMON_HOME* directory. To know all the processes that are using *ORACLE_COMMON_HOME* directory use the following commands:

   On UNIX:

   ```
   ps -ef|grep <oracle_common>
   ```

   On Windows:

Use the Windows Task Manager to identify the processes that use the *ORACLE_COMMON_HOME* directory.

2. Deinstall your Oracle Identity 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 go to the *ORACLE_COMMON_HOME*/oui/bin/ directory (on UNIX) or the *ORACLE_COMMON_HOME*\oui\bin\ directory (on Windows) by running the following command:

   For UNIX:

   ```
   $ cd ORACLE_COMMON_HOME/oui/bin/ directory
   ```

   For Windows:

   ```
   $ cd ORACLE_COMMON_HOME\oui\bin\ directory
   ```

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, as follows:

   On UNIX:

   ```
   ./runInstaller -deinstall -jreLoc FULL_PATH_TO_JRE_DIRECTORY
   ```

   On Windows:

   ```
   setup.exe -deinstall -jreLoc FULL_PATH_TO_JRE_DIRECTORY
   ```

   The Welcome screen appears.

5. Click **Next**. The Select Deinstallation Type screen appears.

6. Select the **Deinstall Oracle Home** option at the top of the Select Deinstallation Type screen.

   Note: The path to the *ORACLE_COMMON_HOME* directory appears in the text describing the **Deinstall Oracle Home** option.

   Click **Next**. The Deinstall Oracle Home screen appears.

7. Confirm the correct *ORACLE_COMMON_HOME* directory is listed, and click **Deinstall**.

   The Deinstallation Progress screen appears, along with a Warning dialog box prompting you to confirm that you want to deinstall the *ORACLE_COMMON_HOME* directory.

8. Click **Yes** on the Warning dialog box to confirm that you want to remove the *ORACLE_COMMON_HOME* directory. The deinstallation begins.

9. Click **Finish** after the deinstallation progresses to 100%. The Deinstallation Complete screen appears.

10. Click **Finish** on the Deinstallation Complete screen to exit the deinstaller.

A.2 Reinstalling Oracle Identity and Access Management

Perform the following steps to reinstall Oracle Identity and Access Management:

1. Verify the directory that 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 11*g* 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.

B Starting or Stopping the Oracle Stack

You must start or stop the components of the Oracle stack in a specific order. Oracle stack refers to Administration Server for the WebLogic Server domain, the system components that are managed by Oracle Process Manager and Notification Server, and the Managed Servers, which are controlled by Node Manager.

This appendix describes that order and contains the following topics:

- Starting the Stack
- Stopping the Stack
- Restarting Servers

Note: When executing the `startManagedWebLogic` and `stopManagedWebLogic` scripts described in the following topics:

- *`SERVER_NAME`* represents the name of the Oracle WebLogic Managed Server, such as `wls_oif1`, `wls_ods1`, or `oam_server1`.
- You will be prompted for values for *`USER_NAME`* and *`PASSWORD`* if you do not provide them as options when you execute the script.
- The value for *`ADMIN_URL`* will be inherited if you do not provide it as an option when you execute the script.

B.1 Starting the Stack

After completing the installation and domain configuration, you must start the Administration Server and various Managed Servers to get your deployments up and running:

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

   On UNIX systems:

   `MW_HOME``/user_projects/domains/`*`domain_name`*`/startWebLogic.sh`

   On Windows systems:

   `MW_HOME``\user_projects\domains\`*`domain_name`*`\startWebLogic.cmd`

   `domain_name` is the name of the domain that you entered on the Specify Domain Name and Location Screen in the Configuration Wizard.

2. Configure Node Manager to start the Managed Servers. If a Managed Server contains other Oracle Fusion Middleware products, such as Oracle SOA Suite, Oracle WebCenter, or Oracle JRF, the Managed Servers environment must be configured to set the correct classpath and parameters. This environment information is provided through the start scripts, such as `startWebLogic` and `setDomainEnv`, which are located in the domain directory.

If the Managed Servers are started by Node Manager (as is the case when the servers are started by the Oracle WebLogic Server Administration Console or Fusion Middleware Control), Node Manager must be instructed to use these start scripts so that the server environments are correctly configured. Specifically, Node Manager must be started with the property `StartScriptEnabled=true`.

There are several ways to ensure that Node Manager starts with this property enabled. As a convenience, Oracle Fusion Middleware provides the following script, which adds the property `StartScriptEnabled=true` to the `nodemanager.properties` file:

On UNIX:

1. Run the following script to add the property `StartScriptEnabled=true` to the `nodemanager.properties` file:

   ORACLE_COMMON_HOME`/common/bin/setNMProps.sh`

2. Start the Node Manager by executing the following command:

   MW_HOME`/WLS_HOME/server/bin/startNodeManager.sh`

On Windows:

1. Run the following script to add the property `StartScriptEnabled=true` to the `nodemanager.properties` file:

   ORACLE_COMMON_HOME`\common\bin\setNMProps.cmd`

2. Start the Node Manager by executing the following command:

   MW_HOME`\WLS_HOME\server\bin\startNodeManager.cmd`

Note: When you start Node Manager, it reads the `nodemanager.properties` file with the `StartScriptEnabled=true` property, and uses the start scripts when it subsequently starts Managed Servers. Note that you need to run the `setNMProps` script only once.

---

3. To start the Managed Servers, run the `startManagedWebLogic.sh` (on UNIX operating systems) or `startManagedWebLogic.cmd` (on Windows operating systems) script in the `bin` directory inside the directory where you created your domain.

Note: If the Node Manager is not running, you can start these Managed Servers from the command line.

This command also requires that you specify a server name. You must start the servers you created when configuring the domain, as shown in the following example:

- `oam_server1` (Oracle Access Manager Server)
- `oim_server1` (Oracle Identity Manager Server)

For example, to start Oracle Access Manager Server on a UNIX system:

```
MW_HOME/user_projects/domains/domain_name/bin/startManagedWebLogic.sh oam_
server1
```

On Windows systems:

```
MW_HOME\user_projects\domains\domain_name\bin\startManagedWebLogic.cmd oam_
server1
```

Before the Managed Server is started, you are prompted for the WebLogic Server user name and password. These were provided on the Configure Administrator Username and Password Screen in the Configuration Wizard.

If the Administration Server is using a non-default port, or resides on a different host than the Managed Servers (in a distributed environment), you must also specify the URL to access the Administration Server.

On UNIX systems:

```
MW_HOME/user_projects/domains/domain_name/bin/startManagedWebLogic.sh oam_
server1 http://host:admin_server_port
```

On Windows systems:

```
MW_HOME\user_projects\domains\domain_name\bin\startManagedWebLogic.cmd oam_
server1 http://host:admin_server_port
```

Instead of being prompted for the Administration Server user name and password, you can also specify them directly from the command lime.

On UNIX systems:

```
MW_HOME/user_projects/domains/domain_name/bin/startManagedWebLogic.sh oam_
server1 http://host:admin_server_port -Dweblogic.management.username=user_name
-Dweblogic.management.password=password
-Dweblogic.system.StoreBootIdentity=true
```

On Windows systems:

```
MW_HOME\user_projects\domains\domain_name\bin\startManagedWebLogic.cmd oam_
server1 http://host:admin_server_port -Dweblogic.management.username=user_name
-Dweblogic.management.password=password
-Dweblogic.system.StoreBootIdentity=true
```

Note: You can use the Oracle WebLogic Administration Console to start managed components in the background. See *Oracle Fusion Middleware Introduction to Oracle WebLogic Server* for more information.

If you do not know the names of the Managed Servers that should be started, you can view the contents of the following file on UNIX systems:

```
MW_HOME/user_projects/domains/domain_name/startManagedWebLogic_readme.txt
```

On Windows systems:

```
MW_HOME\user_projects\domains\domain_name\startManagedWebLogic_readme.txt
```

Or, you can access the Administration Server console at the following URL:

```
http://host:admin_server_port/console
```

Supply the user name and password that you specified on the Configure Administrator Username and Password Screen of the Configuration Wizard. Then, navigate to **Environment > Servers** to see the names of your Managed Servers.

B.2 Stopping the Stack

You can stop the Oracle WebLogic Administration Server and all the managed servers by using Oracle WebLogic Administration Console. See *Oracle Fusion Middleware Introduction to Oracle WebLogic Server* for more information.

To stop the stack components from the command line, perform the following steps:

1. Stop WebLogic managed components, such as Oracle Access Management, Oracle Identity Manager, and Oracle Adaptive Access Manager, by executing the following command:

   ```
   MW_HOME/user_projects/domains/DOMAIN_NAME/bin/stopManagedWebLogic.sh \
   {SERVER_NAME} {ADMIN_URL} {USER_NAME} {PASSWORD}
   ```

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

   ```
   MW_HOME/user_projects/domains/DOMAIN_NAME/bin/stopWebLogic.sh
   ```

3. If you want to stop the Node Manager, use the `kill` command:

   ```
   kill -9 PID
   ```

B.3 Restarting Servers

To restart the Administration Server or Managed Servers, you must stop running Administration Server or Managed Servers first before starting them again. For more information, see Stopping the Stack and Starting the Stack.