# Oracle® Fusion Middleware

Upgrade and Migration Guide for Oracle Identity and Access Management

11*g* Release 2 (11.1.2)

**E28183-13**

August 2014

Documentation for Oracle Fusion Middleware administrators who want to upgrade or migrate to Oracle Identity and Access Management 11*g* Release 2 (11.1.2).

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

E28183-13

Primary Author: Shynitha K S

Contributing Author: Wortimla R S

Contributors: Allison Sparshott, Arun Singla, Aruna Vempaty, Ashish Gupta, Ashwini Singhvi, Ayush Jindal, Ballaji Sahoo, Bhavik Sankesara, Brad Donnison, Bruce Xie, Charles Wesley, Deepak Ramakrishnan, Derick Leo, Gaurav Johar, Gaurav Srivastava, Gururaj B S, Kavita Tippanna, Kishor Negi, Kumar Dhanagopal, Lixin Zheng, Lokesh Gupta, Madhu Martin, Mark Karlstrand, Mark Wilcox, Mrudul Uchil, Nagasravani Akula, Neelanand Sharma, Niranjan Ananthapadmanabha, Pallavi Rao, Peter Laquerre, Raminder Deep Kaler, Ramya Subramanya, Ravi Thirumalasetty, Rubis Chowallur, Sandeep Dongare, Sanjay Sadarangani, Sanjeev Sharma, Semyon Shulman, Sitaraman Swaminathan, Sree Chitturi, Srinivas Nagandla, Stephen Mathew, Steven Frehe, Stuart Duggan, Sumeet Agarwal, Svetlana Kolomeyskaya, Tushar Wagh, Umesh Waghode, Vadim Lander, Vishal Mishra, Venu Shastri, William Cai

# Contents

## 5 Upgrading Oracle Adaptive Access Manager 11*g* Release 1 (11.1.1.5.0) Environments

## 6 Upgrading Oracle Identity Manager 11*g* Release 1 (11.1.1.5.0) Environments

## 7 Upgrading Oracle Entitlements Server 11*g* Release 1 (11.1.1.5.0) Environments

## 8 Upgrading Oracle Identity Navigator 11*g* Release 1 (11.1.1.5.0) Environments

## 9 Upgrading Oracle Identity and Access Management 11*g* Release1 (11.1.1.3.0) Environments

## 10 Upgrading Oracle Identity Manager 9.x Environments

## Part III Migrating Various Oracle 10*g* and OpenSSO Environments

## 11 Migration and Coexistence Starting Points

## 12 Migrating Oracle Access Manager 10*g* Environments

## 15 Migrating Sun OpenSSO Enterprise 8.0 Environments

## 16 Migrating Sun Java System Access Manager 7.1 Environments

## 17 Coexistence of Oracle Access Manager 10*g* with Oracle Access Management Access Manager 11.1.2

## 18 Coexistence of Sun OpenSSO Enterprise 8.0 with Oracle Access Management Access Manager 11.1.2

## 19 Coexistence of Sun Java System Access Manager 7.1 with Oracle Access Management Access Manager 11.1.2

# Preface

This document describes how to upgrade or migrate to Oracle Identity and Access Management 11*g* Release 2 (11.1.2) products.

## Audience

This document is intended for administrators who are responsible for upgrading or migrating to Oracle Identity and Access Management 11*g* Release 2 (11.1.2).

## 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

For more information, see the following documents in the Oracle Identity and Access Management 11*g* Release 2 (11.1.2) documentation library:

- *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Entitlements Server*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Navigator*
- *Oracle Fusion Middleware High Availability Guide*
- *Oracle Fusion Middleware Release Notes*

## 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

# Understanding Oracle Identity and Access Management

This part includes the following chapters:

- Chapter 1, "Introduction"
- Chapter 2, "Documentation Roadmap"

# 1 Introduction

This chapter provides an overview of Oracle Identity and Access Management 11*g* Release 2 (11.1.2) products. This chapter includes the following topics:

- Oracle Identity and Access Management Overview
- Upgrade Scenarios
- Migration and Coexistence Scenarios

## 1.1 Oracle Identity and Access Management Overview

Oracle Identity and Access Management components enable enterprises to manage the end-to-end lifecycle of user identities across all enterprise resources - both within and beyond the firewall. With Oracle Identity and Access Management, you can deploy applications faster, apply the most granular protection to enterprise resources, automatically eliminate latent access privileges, and much more.

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

- Oracle Identity Manager
- Oracle Access Management, which includes the following components:
  - Oracle Access Management Access Manager
  - Oracle Access Management Identity Federation
  - Oracle Access Management Mobile and Social
  - Oracle Access Management Security Token Service
- Oracle Adaptive Access Manager
- Oracle Identity Navigator
- Oracle Entitlements Server
- Oracle Privileged Account Manager

## 1.2 Upgrade Scenarios

The term **Upgrade** in this document refers to the upgrade of existing Oracle Identity and Access Management 11*g* Release 1 components to Oracle Identity and Access Management 11*g* Release 2 (11.1.2). For each of these upgrade scenarios, you use the Oracle Identity and Access Management 11*g* Release 2 (11.1.2) installer to update your existing Oracle Home (*`IAM_HOME`*) to Oracle Identity and Access Management 11*g* Release 2 (11.1.2).

You can upgrade the following Oracle Identity and Access Management components to Oracle Identity and Access Management 11.1.2:

- Oracle Identity Manager 11.1.1.5.0
- Oracle Access Manager 11.1.1.5.0
- Oracle Adaptive Access Manager 11.1.1.5.0
- Oracle Identity Navigator 11.1.1.5.0
- Oracle Entitlements Server 11.1.1.5.0
- Oracle Identity Manager 11.1.1.3.0
- Oracle Access Manager 11.1.1.3.0
- Oracle Adaptive Access Manager 11.1.1.3.0
- Oracle Identity Navigator 11.1.1.3.0
- Oracle Identity Manager 9.x

## 1.3 Migration and Coexistence Scenarios

The term **Migration** in this document refers to the scenarios where you migrate the following products to Oracle Identity and Access Management 11*g* Release 2 (11.1.2). In these migration scenarios, you install a new 11*g* Release 2 (11.1.2) Oracle Home (*IAM_HOME*) and then migrate your configuration data from your previous installation to the new 11*g* Release 2 (11.1.2) Oracle Home.

- Oracle Access Manager 10*g*
- Oracle Adaptive Access Manager 10*g*
- Oracle Single Sign-On 10*g*
- Sun OpenSSO Enterprise 8.0
- Sun Java System Access Manager 7.1

During migration, you can have both the old and the new deployments coexisting, such that some applications are protected by the old server, and the others are protected by the new server. The coexistence mode allows you to have seamless single sign-on experience when you navigate between applications protected by different servers.

For example, Sun OpenSSO Enterprise 8.0 and Oracle Access Management Access Manager 11.1.2 servers can coexist and work together, so that the you have seamless single sign-on experience when you navigate between applications protected by Sun OpenSSO Enterprise 8.0 and Oracle Access Management Access Manager 11.1.2 Servers.

The following are the coexistence scenarios supported in 11*g* Release 2 (11.1.2):

- Coexistence of Oracle Access Manager 10*g* with Oracle Access Management Access Manager 11.1.2
- Coexistence of Sun OpenSSO Enterprise 8.0 with Oracle Access Management Access Manager 11.1.2
- Coexistence of Sun Java System Access Manager 7.1 with Oracle Access Management Access Manager 11.1.2

# 2 Documentation Roadmap

This chapter describes the lists the upgrade, migration, and coexistence scenarios for Oracle Identity and Access Management 11*g* Release 2 (11.1.2). Depending on the scenario, go to the respective chapter, and follow the procedure.

> **Note:** For more information about the upgrade, migration, and coexistence scenarios, see Chapter 1, "Introduction".

Table 2–1 lists the upgrade, migration, and coexistence scenarios for Oracle Identity and Access Management 11.1.2.

***Table 2–1 Roadmap***

| Topic | Description |
|---|---|
| Upgrade Scenarios | See<br>Chapter 4, "Upgrading Oracle Access Manager 11g Release 1 (11.1.1.5.0) Environments"<br>Chapter 5, "Upgrading Oracle Adaptive Access Manager 11g Release 1 (11.1.1.5.0) Environments"<br>Chapter 6, "Upgrading Oracle Identity Manager 11g Release 1 (11.1.1.5.0) Environments"<br>Chapter 8, "Upgrading Oracle Identity Navigator 11g Release 1 (11.1.1.5.0) Environments"<br>Chapter 7, "Upgrading Oracle Entitlements Server 11g Release 1 (11.1.1.5.0) Environments"<br>Chapter 9, "Upgrading Oracle Identity and Access Management 11g Release1 (11.1.1.3.0) Environments"<br>Chapter 10, "Upgrading Oracle Identity Manager 9.x Environments" |
| Migration Scenarios | See<br>Chapter 12, "Migrating Oracle Access Manager 10g Environments"<br>Chapter 13, "Migrating Oracle Adaptive Access Manager 10g Environments"<br>Chapter 14, "Migrating Oracle Single Sign-On 10g Environments"<br>Chapter 15, "Migrating Sun OpenSSO Enterprise 8.0 Environments"<br>Chapter 16, "Migrating Sun Java System Access Manager 7.1 Environments" |

*Table 2–1 (Cont.) Roadmap*

| Topic | Description |
|---|---|
| Coexistence Scenarios | See,<br>Chapter 17, "Coexistence of Oracle Access Manager 10g with Oracle Access Management Access Manager 11.1.2"<br>Chapter 18, "Coexistence of Sun OpenSSO Enterprise 8.0 with Oracle Access Management Access Manager 11.1.2"<br>Chapter 19, "Coexistence of Sun Java System Access Manager 7.1 with Oracle Access Management Access Manager 11.1.2" |

# Part II

# Upgrading Oracle Identity and Access Management 11.1.1.5.0 and 11.1.1.3.0 Environments

This part includes the following chapters:

- Chapter 3, "Upgrade Starting Points"
- Chapter 4, "Upgrading Oracle Access Manager 11g Release 1 (11.1.1.5.0) Environments"
- Chapter 5, "Upgrading Oracle Adaptive Access Manager 11g Release 1 (11.1.1.5.0) Environments"
- Chapter 6, "Upgrading Oracle Identity Manager 11g Release 1 (11.1.1.5.0) Environments"
- Chapter 7, "Upgrading Oracle Entitlements Server 11g Release 1 (11.1.1.5.0) Environments"
- Chapter 8, "Upgrading Oracle Identity Navigator 11g Release 1 (11.1.1.5.0) Environments"
- Chapter 9, "Upgrading Oracle Identity and Access Management 11g Release1 (11.1.1.3.0) Environments"
- Chapter 10, "Upgrading Oracle Identity Manager 9.x Environments"

# 3

# Upgrade Starting Points

This chapter describes the supported starting points for Oracle Identity and Access Management upgrade.

This chapter contains the following sections:

- Supported Starting Points for Oracle Access Manager 11.1.1.5.0
- Supported Starting Points for Oracle Adaptive Access Manager 11.1.1.5.0
- Supported Starting Points for Oracle Identity Manager 11.1.1.5.0
- Supported Starting Points for Oracle Entitlements Server 11.1.1.5.0
- Supported Starting Points for Oracle Identity and Access Management 11.1.1.3.0
- Supported Starting Points for Oracle Identity Manager 9.x

> **Note:** The patch sets listed in this chapter are the latest patch sets available at the time this guide was published.
>
> For a list of the latest patch sets available for your installation, visit *My Oracle Support*.

For more information on upgrade scenarios, see Section 1.2, "Upgrade Scenarios,".

## 3.1 Supported Starting Points for Oracle Access Manager 11.1.1.5.0

Table 3–1 lists the supported starting points for upgrading Oracle Access Manager 11*g* Release 1 (11.1.1.5.0) to Oracle Access Management Access Manager 11*g* Release 2 (11.1.2):

***Table 3–1 Oracle Access Manager 11.1.1.5.0 Releases***

| Release | Supported Bundle Patch |
|---|---|
| 11*g* Release 1 (11.1.1.5.0) | ■ Bundle Patch 11.1.1.5.1<br>■ Bundle Patch 11.1.1.5.2 |

## 3.2 Supported Starting Points for Oracle Adaptive Access Manager 11.1.1.5.0

Table 3–2 lists the supported starting points for upgrading Oracle Adaptive Access Manager 11*g* Release 1 (11.1.1.5.0) to Oracle Adaptive Access Manager 11*g* Release 2 (11.1.2):

***Table 3–2 Oracle Adaptive Access Manager 11.1.1.5.0 Releases***

| Release | Supported Bundle Patch |
|---|---|
| 11*g* Release 1 (11.1.1.5.0) | ▪ Bundle Patch 11.1.1.5.1<br>▪ Bundle Patch 11.1.1.5.2 |

## 3.3 Supported Starting Points for Oracle Identity Manager 11.1.1.5.0

Table 3–3 lists the supported starting points for upgrading Oracle Identity Manager 11*g* Release 1 (11.1.1.5.0) to Oracle Identity Manager 11*g* Release 2 (11.1.2):

***Table 3–3 Oracle Identity Manager 11.1.1.5.0 Releases***

| Release | Supported Bundle Patch |
|---|---|
| 11*g* Release 1 (11.1.1.5.0) | ▪ All Bundle Patches are supported |

## 3.4 Supported Starting Points for Oracle Entitlements Server 11.1.1.5.0

Table 3–4 lists the supported starting points for upgrading Oracle Entitlements Server 11*g* Release 1 (11.1.1.5.0) to Oracle Entitlements Server 11*g* Release 2 (11.1.2):

***Table 3–4 Oracle Entitlements Server 11.1.1.5.0 Releases***

| Release | Supported Bundle Patch |
|---|---|
| 11*g* Release 1 (11.1.1.5.0) | ▪ Bundle Patch 11.1.1.5.1 |

## 3.5 Supported Starting Points for Oracle Identity and Access Management 11.1.1.3.0

Table 3–5 lists the supported starting points for upgrading Oracle Identity and Access Management 11*g* Release 1 (11.1.1.5.0) to Oracle Identity and Access Management 11*g* Release 2 (11.1.2):

***Table 3–5 Oracle Identity and Access Management 11.1.1.3.0 Releases***

| Release | Supported Components |
|---|---|
| 11*g* Release 1 (11.1.1.3.0) | ▪ Oracle Access Manager 11.1.1.3.0<br>▪ Oracle Adaptive Access Manager 11.1.1.3.0<br>▪ Oracle Identity Manager 11.1.1.3.0<br>▪ Oracle Identity Navigator 11.1.1.3.0 |

## 3.6 Supported Starting Points for Oracle Identity Manager 9.x

Table 3–6 lists the supported starting points for upgrading Oracle Identity Manager 9.x to Oracle Identity Manager 11*g* Release 2 (11.1.2):

***Table 3–6 Oracle Identity Manager 9.x Releases***

| Release | Supported Bundle Patch |
|---|---|
| Oracle Identity Manager 9.x | ▪ All Bundle Patches are supported |

# 4 Upgrading Oracle Access Manager 11*g* Release 1 (11.1.1.5.0) Environments

This chapter describes how to upgrade your existing Oracle Access Manager 11*g* Release 1 (11.1.1.5.0) environment to Oracle Access Management Access Manager (Access Manager) 11*g* Release 2 (11.1.2).

This chapter contains the following sections:

- Upgrade Roadmap for Oracle Access Manager
- Shutting Down Administration Server and Managed Servers
- Backing Up Oracle Access Manager 11g Release 1 (11.1.1.5.0)
- Optional: Upgrading Oracle WebLogic Server
- Creating Oracle Access Management Access Manager Schemas Using Repository Creation Utility
- Upgrading Oracle Access Manager 11g Release 1 (11.1.1.5.0) to Oracle Access Management Access Manager 11g Release 2 (11.1.2)
- Extending Oracle Access Manager 11.1.1.5.0 Component Domains with Oracle Platform Security Services Template
- Upgrading Oracle Platform Security Services
- Configuring Oracle Platform Security ServicesSecurity Store
- Exporting Access Data
- Importing Access Data
- Starting the Administration Server and Access Manager Managed Servers
- Redeploying Oracle Access Management Access Manager Servers and Shared Libraries
- Stopping the Administration Server and Access Manager Managed Servers
- Deleting Folders
- Starting the Administration Server and Access Manager Managed Servers
- Verifying the Upgrade
- Troubleshooting

Read the Oracle Fusion Middleware System Requirements and Specifications document to ensure that your environment meets the minimum requirements for the products you are installing or upgrading.

## 4.1 Upgrade Roadmap for Oracle Access Manager

**Note:** If you do not follow the exact sequence provided in this task table, your Oracle Access Manager upgrade may not be successful.

Table 4–1 lists the steps to upgrade Oracle Access Manager 11.1.1.5.0.

***Table 4–1 Upgrade Flow***

| Task No. | Task | For More Information |
|---|---|---|
| 1 | Shut down all servers. This includes both Administration Server and Managed Servers. | See, Shutting Down Administration Server and Managed Servers |
| 2 | Back up your environment. | See, Backing Up Oracle Access Manager 11g Release 1 (11.1.1.5.0) |
| 3 | Optional - Upgrade Oracle WebLogic Server 10.3.5 to Oracle WebLogic Server 10.3.6. | See, Optional: Upgrading Oracle WebLogic Server |
| 4 | Run Oracle Fusion Middleware Repository Creation Utility (RCU) to create and load Access Manager schemas and OPSS schema. | See, Creating Oracle Access Management Access Manager Schemas Using Repository Creation Utility |
| 5 | Upgrade 11.1.1.5.0 Oracle Home to 11.1.2. | See, Upgrading Oracle Access Manager 11g Release 1 (11.1.1.5.0) to Oracle Access Management Access Manager 11g Release 2 (11.1.2) |
| 6 | Extend your Oracle Access Manager 11.1.1.5.0 domain with the OPSS template. | See, Extending Oracle Access Manager 11.1.1.5.0 Component Domains with Oracle Platform Security Services Template |
| 7 | Upgrade Oracle Platform Security Services. | See, Upgrading Oracle Platform Security Services |
| 8 | Run the `configuresecuritystore.py` script to configure policy stores. | See, Configuring Oracle Platform Security ServicesSecurity Store |
| 9 | Export access data. | See, Exporting Access Data |
| 10 | Import access data. | See, Importing Access Data |
| 11 | Start the Administration Server and Oracle Access Management Access Manager Managed Servers. | See, Starting the Administration Server and Access Manager Managed Servers |
| 12 | Redeploy Access Manager servers and shared libraries. | See, Redeploying Oracle Access Management Access Manager Servers and Shared Libraries |
| 13 | Stop the Administration Server and Oracle Access Management Access Manager Managed Server. | See, Stopping the Administration Server and Access Manager Managed Servers |
| 14 | Delete the `tmp` and `stage` folders. | See, Deleting Folders |
| 15 | Start the Administration Server and Oracle Access Management Access Manager Managed Servers. | See, Starting the Administration Server and Access Manager Managed Servers |
| 16 | Verify the Access Manager upgrade. | See, Verifying the Upgrade |

## 4.2 Shutting Down Administration Server and Managed Servers

The upgrade process involves changes to the binaries and to the schema. Therefore, before you begin the upgrade process, you must shut down the Administration Server and Managed Servers.

To shut down the Servers, do the following:

### Stopping the Administration Server

To stop the Administration Server, do the following:

**On UNIX**:

Run the following command:

```
cd <MW_HOME>/user_projects/domains/<domain_name>/bin
```

```
./stopWebLogic.sh
```

**On Windows**:

Run the following command:

```
cd <MW_HOME>\user_projects\domains\<domain_name>\bin
```

```
stopWebLogic.cmd
```

### Stopping Managed Servers

To stop the Managed Servers, do the following:

**On UNIX**:

1. Move from your present working directory to the `<MW_HOME>/user_projects/domains/<domain_name>/bin` directory by running the following command on the command line:

   ```
   cd <MW_HOME>/user_projects/domains/<domain_name>/bin
   ```

2. Run the following command to stop the servers:

   ```
   ./stopManagedWebLogic.sh <server_name> <admin_url> <user_name>
   <password>
   ```

   where

   `<server_name>` is the name of the Managed Server.

   `<admin_url>` is URL of the WebLogic administration console. Specify it in the format `http://<host>:<port>/console`. Specify only if the WebLogic Administration Server is on a different computer.

   `<user_name>` is the username of the WebLogic Administration Server.

   `<password>` is the password of the WebLogic Administration Server.

**On Windows**:

1. Move from your present working directory to the `<MW_HOME>\user_projects\domains\<domain_name>\bin` directory by running the following command on the command line:

   ```
   cd <MW_HOME>\user_projects\domains\<domain_name>\bin
   ```

2. Run the following command to stop the Managed Servers:

   ```
   stopManagedWebLogic.cmd <server_name> <admin_url> <username> <password>
   ```

where

`<server_name>` is the name of the Managed Server.

`<admin_url>` is URL of the WebLogic administration console. Specify it in the format `http://<host>:<port>/console`. specify only if the WebLogic Administration Server is on a different computer.

`<username>` is the username of the WebLogic Administration Server.

`<password>` is the password of the WebLogic Administration Server.

For more information, see "Stopping the Stack" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

## 4.3 Backing Up Oracle Access Manager 11*g* Release 1 (11.1.1.5.0)

You must back up your Oracle Access Manager 11.1.1.5.0 environment before you upgrade to Access Manager 11.1.2.

After stopping the servers, back up the following:

- *MW_HOME* directory, including the Oracle Home directories inside Middleware Home
- Domain Home directory
- Oracle Access Manager schemas
- MDS schemas
- Audit and any other dependent schemas

## 4.4 Optional: Upgrading Oracle WebLogic Server

**Note:** Upgrading Oracle WebLogic Server is not mandatory. However, Oracle recommends that you upgrade Oracle WebLogic Server to 10.3.6.

You can upgrade WebLogic Server 10.3.5 to Oracle WebLogic Server 10.3.6 by using the WebLogic 10.3.6 Upgrade Installer. Complete the following steps:

1. Download the WebLogic 10.3.6 Upgrade Installer from Oracle Technology Network.

   For more information, see "Downloading the Installer From Oracle Technology Network" in the *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*.

2. Run the Upgrade Installer in graphical mode to upgrade your WebLogic Server.

   For more information, see "Running the Upgrade Installer in Graphical Mode" in the *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*.

## 4.5 Creating Oracle Access Management Access Manager Schemas Using Repository Creation Utility

Upgrading Oracle Access Manager 11.1.1.5.0 schema to Oracle Access Management Access Manager 11.1.2 is not supported. You cannot update Oracle Access Manager

11.1.1.5.0 schemas to Access Manager 11.1.2, so, you must create new Access Manager 11.1.2 schemas.

Run Repository Creation utility (RCU) to create the Access Manager schema. Select all dependent schemas so that OPSS schema gets created too.

For more information, see "Creating Schemas" in the *Using Repository Creation Utility*.

> **Note:** Even if you are creating new schemas, do not delete your Oracle Access Manager 11.1.1.5.0 schemas and do not use the old schema name, as you will need the old schema credentials while "Exporting Access Data".

## 4.6 Upgrading Oracle Access Manager 11*g* Release 1 (11.1.1.5.0) to Oracle Access Management Access Manager 11*g* Release 2 (11.1.2)

To upgrade Oracle Access Manager, you must use the 11.1.2 installer. During the procedure, point the Middleware Home to your existing 11.1.1.5.0 Oracle Access Manager Middleware Home. Your Oracle Home is upgraded from 11.1.1.5.0 to 11.1.2.

This section contains the following topics:

- Obtaining the Software
- Starting the Oracle Identity and Access Management 11g Release 2 (11.1.2) Installer
- Installing Oracle Identity and Access Management 11g Release 2 (11.1.2)

### 4.6.1 Obtaining the Software

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

### 4.6.2 Starting the Oracle Identity and Access Management 11*g* Release 2 (11.1.2) Installer

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

> **Notes:**
>
> - If you are installing 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 doing the following:

**On UNIX**:

1. Move from your present working directory to the directory where you extracted the contents of the Installer to.
2. Move to the following location:

   ```
   cd Disk1
   ```

3. Run the following command:

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

For example:

```
./runInstaller -jreLoc <MW_HOME>/jdk160_29/jre
```

**On Windows**:

1. Move from your present working directory to the directory where you extracted the contents of the Installer to.
2. Move to the following location:

   ```
   cd Disk1
   ```

3. Run the following command:

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

   For Example:

   ```
   setup.exe -jreLoc <MW_HOME>\jdk160_29\jre
   ```

---

**Note:** 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 is not created in your Middleware Home. You must enter the absolute path to the JRE folder from where your JDK is located.

---

### 4.6.3 Installing Oracle Identity and Access Management 11*g* Release 2 (11.1.2)

Use the Oracle Identity and Access Management 11.1.2 Installer to upgrade Oracle Access Manager 11.1.1.5.0 to Access Manager 11.1.2:

1. After you start the Installer, the **Welcome** screen appears.
2. Click **Next** on the **Welcome** screen. The **Install Software Updates** screen appears. Select whether or not you want to search for updates. Click **Next**.
3. The **Prerequisite Checks** screen appears. If all prerequisite checks pass inspection, click **Next**. The **Specify Installation Location** screen appears.
4. On the **Specify Installation Location** screen, point the Middleware Home to your existing 11.1.1.5.0 Middleware Home installed on your system.
5. In the **Oracle Home Directory** field, specify the path of the existing Oracle Identity and Access Management Home. This directory is also referred to as `<IAM_HOME>` in this book.

   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 you want to proceed with 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 **Help** on the installation wizard screens.

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

   This installation process copies the 11.1.2 Oracle Identity and Access Management software to your system.

For more information, see "Installing and Configuring Oracle Identity and Access Management (11.1.2)" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

## 4.7 Extending Oracle Access Manager 11.1.1.5.0 Component Domains with Oracle Platform Security Services Template

Oracle Access Management Access Manager 11.1.2 uses the database to store policies. This requires extending Oracle Access Manager 11.1.1.5.0 domain to include the OPSS data source.

To extend your Oracle Access Manager 11.1.1.5.0 component domain with the OPSS template, complete the following steps:

1. Run the following command:

   **On UNIX:**

   ```
   ./config.sh
   ```

   It is located in the `<MW_HOME>/<Oracle_IDM1>/common/bin` directory.

   **On Windows:**

   ```
   config.cmd
   ```

   It is located in the `<MW_HOME>\<Oracle_IDM1>\common\bin` directory.

2. On the **Welcome** screen, select the **Extend an existing WebLogic domain** option. Click **Next**.
3. On the **Select a WebLogic Domain Directory** screen, browse to the directory that contains the WebLogic domain in which you configured Oracle Access Manager. Click **Next**. The **Select Extension Source** screen appears.
4. On the **Select Extension Source** screen, select the **Oracle Platform Security Service - 11.1.1.0 [Oracle_IDM1]** option. After selecting the domain configuration options, click **Next**.
5. The **Configure JDBC Data Sources** screen appears. Update the component schemas: Access Manager Infrastructure and OPSS schema. Configure Access Manager Infrastructure, by updating the older Oracle Access Manager 11.1.1.5.0 schema information shown in the screen, with new Access Manager 11.1.2 schema details and OPSS schema data source. After the test succeeds, the **Configure JDBC Component Schema** screen appears.

6. On the **Configure JDBC Component Schema** screen, select **Oracle Platform Security Services**.

   Set values for Schema Owner, Schema Password, Database and Service, Host Name, and Port. Click **Next**.

   The **Test JDBC Component Schema** screen appears. After the test succeeds, the **Select Optional Configuration** screen appears.

7. On the **Select Optional Configuration** screen, you can configure Managed Servers, Clusters, and Machines and Deployments and Services. Do not select anything as you have already configured your Oracle Access Manager 11.1.1.5.0 environment. Click **Next**.

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

Your existing Oracle Access Manager domain is extended to support Oracle Platform Security Services (OPSS), and Oracle Access Manager is configured to use the newly created 11.1.2 OPSS policy schema.

## 4.8 Upgrading Oracle Platform Security Services

To upgrade Oracle Platform Security Services (OPSS) schema, do the following:

### On UNIX:

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

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

2. Run the following command to launch the WebLogic Scripting Tool (WLST):

   ```
   ./wlst.sh
   ```

3. At the WLST prompt, run the following command:

   ```
   upgradeOpss(jpsConfig="existing_jps_config_file", jaznData="system_
   jazn_data_file")
   ```

   For example:

   ```
   upgradeOpss(jpsConfig="<MW_HOME>/user_projects/domains/base_
   domain/config/fmwconfig/jps-config.xml",jaznData="<MW_HOME>/oracle_
   common/modules/oracle.jps_11.1.1/domain_config/system-jazn-data.xml")
   ```

4. Exit the WLST console using the `exit()`command.

### On Windows:

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

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

2. Run the following command to launch the WebLogic Scripting Tool (WLST):

   ```
   wlst.cmd
   ```

3. At the WLST prompt, run the following command:

```
upgradeOpss(jpsConfig="existing_jps_config_file", jaznData="system_
jazn_data_file")
```

For example:

```
upgradeOpss(jpsConfig="<MW_HOME>\\user_projects\\domains\\base_
domain\\config\\fmwconfig\\jps-config.xml",jaznData="<MW_HOME>\\oracle_
common\\modules\\oracle.jps_11.1.1\\domain_
config\\system-jazn-data.xml")
```

4. Exit the WLST console using the `exit()` command.

Table 4–2 describes the parameters you need to specify on the command line:

***Table 4–2 Parameters for Upgrading OPSS***

| Parameter | Description |
|---|---|
| `jpsConfig` | Specify the path to the `jps-config.xml` file in your Access Manager 11.1.2 installation. The following example shows the complete path:<br>On UNIX, it is located in the `<MW_HOME>/user_projects/domains/base_domain/config/fmwconfig/jps-config.xml` directory.<br>On Windows, it is located in the `<MW_HOME>\user_projects\domains\base_domain\config\fmwconfig\jps-config.xml directory.` |
| `jaznData` | Specify the path to the `system-jazn-data.xml` file in your Access Manager 11.1.2 installation. The following example shows the complete path:<br>On UNIX, it is located in the `<MW_HOME>/oracle_common/modules/oracle.jps_11.1.1/domain_config/system-jazn-data.xml` directory.<br>On Windows, it is located in the `<MW_HOME>\oracle_common\modules\oracle.jps_11.1.1\domain_config\system-jazn-data.xml` directory. |

## 4.9 Configuring Oracle Platform Security ServicesSecurity Store

You must configure the Database Security Store as it is the only security store type supported by Oracle Identity and Access Management 11g Release 2 (11.1.2).

For more information on configuring Oracle Platform Security Services, see "Configuring Database Security Store for an Oracle Identity and Access Management Domain" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

## 4.10 Exporting Access Data

Policy information from Oracle Access Manager 11.1.1.5.0 schema needs to be extracted before importing it to the Access Manager 11.1.2 schema. The `exportAccessData` WLST command exports the Access Manager policy and configuration information from the 11.1.1.5.0 Oracle Access Manager domain. You must export Oracle Access Manager 11.1.1.5.0 configuration details, policy stores, keys, and CSF Passwords.

Complete the following steps to export data:

### On UNIX:

1. Move from your present working directory to the `<IAM_HOME>/common/bin` directory by running the following command on the command line:

   ```
   cd <IAM_HOME>/common/bin
   ```

2. Run the following command to launch the WebLogic Scripting Tool (WLST):

   ```
   ./wlst.sh
   ```

3. At the WLST prompt, run the following script:

   ```
   exportAccessData("<UPGRADE_PROPERTIES_FILE>")
   ```

   For example:

   ```
   exportAccessData("<IAM_HOME>/oam/server/wlst/scripts/sample_
   properties/oam_upgrade.properties")
   ```

   See Table 4–4 for sample properties and description.

4. Exit the WLST console using the `exit()` command.

### On Windows:

1. Move from your present working directory to the `<IAM_HOME>\common\bin` directory by running the following command on the command line:

   ```
   cd <IAM_HOME>\common\bin
   ```

2. Run the following command to launch the WebLogic Scripting Tool (WLST):

   ```
   wlst.cmd
   ```

3. At the WLST prompt, run the following script:

   ```
   exportAccessData("<UPGRADE_PROPERTIES_FILE>")
   ```

   For example:

   ```
   exportAccessData("<IAM_HOME>\\oam\\server\\wlst\\scripts\\sample_
   properties\\oam_upgrade.properties")
   ```

   See Table 4–4 for sample properties and description.

4. Exit the WLST console using the `exit()` command.

Table 4–3 describes the parameters you must specify on the command line:

***Table 4–3 Parameters for Exporting Data***

| Parameter | Description |
|---|---|
| `properties_location` | Specify the path to the `oam_upgrade.properties` file in the Access Manager 11.1.1.5.0 installation. The following example shows the complete path:<br>On UNIX, it is located in the `<IAM_HOME>/oam/server/wlst/scripts/sample_properties/oam_upgrade.properties` directory.<br>On Windows, it is located in the `<IAM_HOME>\oam\server\wlst\scripts\sample_properties\oam_upgrade.properties` directory. |

Table 4–4 lists the properties of `oam_upgrade.properties`:

*Table 4–4 Property Description*

| Properties | Description |
|---|---|
| MW_HOME | Specify the complete path to the Middleware Home. The following example shows the complete path:<br>On UNIX, it is located in the Oracle/Middleware directory.<br>On Windows, it is located in the Oracle\Middleware directory. |
| IAM_HOME | Specify the complete path to the Oracle Identity and Access Management location. The following example shows the complete path:<br>On UNIX, it is located in the <MW_HOME>/<Oracle_IDM1> directory.<br>On Windows, it is located in the <MW_HOME>\<Oracle_IDM1> directory. |
| ORACLE_HOME | This property refers to the location of the Oracle Identity and Access Management software. The following example shows the complete path:<br>On UNIX, it is located in the <MW_HOME>/<IAM_HOME> directory.<br>On Windows, it is located in the <MW_HOME>\<IAM_HOME> directory. |
| OAM_DOMAIN_HOME | This property refers to the existing Oracle Access Manager 11.1.1.5.0 domain home. The following example shows the complete path:<br>On UNIX, it is located in the <MW_HOME>/user_projects/domains/<oam_domain> directory.<br>On Windows, it is located in the <MW_HOME>\user_projects\domains\<oam_domain> directory. |
| ORACLE_COMMON_HOME | This property refers to the common components home. The following example shows the complete path:<br>On UNIX, it is located in the <MW_HOME>/Oracle_Common directory.<br>On Windows, it is located in the <MW_HOME>\Oracle_Common directory. |
| OAM_DEST_ARTIFACTS_LOCATION | This property refers to the location where you want to place the upgrade artifacts, such as Oracle Access Manager 11.1.1.5.0 configuration and policy files. |
| OAM_TYPE_OF_UPGRADE | This is an InPlace upgrade. |
| OAM_IS_INCREMENTAL | This property is used to specify if you run the upgrade in an incremental mode.<br>Incremental form of upgrade is not supported in Access Manager 11.1.2. Therefore, set the value as False. |
| OAM_POLICY_UPGRADE_OPTIMIZATION | As a part of the Oracle Access Manager policy upgrade, the changes to the out of the box Access Manager policies are applied on top of the existing (11.1.1.5.0) out of the box policies. This process involves a three way merge of the Access Manager policies. This is a time consuming process (takes about 30 minutes).<br>If you want to proceed with the merge, set the property to False.<br>If you want to replace the Oracle Access Manager 11.1.1.5.0 out of the box policies with the new ones, without the merge process, set this property to True. |

*Table 4–4 (Cont.) Property Description*

| Properties | Description |
|---|---|
| `OAM_PS1_SCHEMA_OWNER` | Use this property to connect to the 11.1.1.5.0 policy store. Specify the Oracle Access Manager 11.1.1.5.0 schema owner. |
| `OAM_PS1_SCHEMA_CRED` | Use this property to connect to the 11.1.1.5.0 policy store. Specify the Oracle Access Manager 11.1.1.5.0 schema credentials. |
| `OAM_PS1_CREDENTIAL_ALIAS` | Use this property to connect to the 11.1.1.5.0 policy store. Specify the Oracle Access Manager 11.1.1.5.0 Oracle Entitlements Server database credential alias as:<br>`OESDBCredentialAlias` |
| `OAM_PS1_JDBC_CONN_STRING` | Use this property to connect to the 11.1.1.5.0 policy store. Specify the JDBC connection string in the following format:<br>`jdbc:oracle:thin:@dbhost:dbport/sid` |
| `OAM_PS1_JDBC_DRIVER_CLASS` | Use this property to connect to the 11.1.1.5.0 policy store. Specify the JDBC driver class in the following format:<br>`oracle.jdbc.OracleDriver` |
| `OAM_PS1_ROOT_DN` | Use this property to connect to the 11.1.1.5.0 policy store. Specify the properties as:<br>`cn=farm,cn=JPSContext,cn=jpsroot` |
| `OAM_PS1_POLICY_FILE` | This property refers to the absolute path to the XML file where extracted 11.1.1.5.0 policy needs to be saved. Specify the path where you want to save the extracted Oracle Access Manager 11.1.1.5.0 policies.<br>For example:<br>On UNIX, specify the following path:<br>`OAM_PS1_POLICY_FILE=<UPGRADE_ATRIFACTS_DIR>/oam-policy-ps1.xml`<br>On Windows, specify the following path:<br>`OAM_PS1_POLICY_FILE=<UPGRADE_ATRIFACTS_DIR>\oam-policy-ps1.xml` |
| `OAM_PS1_POLICY_JARS` | Upgrade frameworks loads version specific jars for Exporting and Importing data. This property refers to the Oracle Access Manager 11.1.1.5.0 policy jars available at the following path:<br>On UNIX, it is located in the `$<ORACLE_HOME>/oam/server/lib/upgrade/ps1-policy` directory.<br>On Windows, it is located in the `<ORACLE_HOME>\oam\server\lib\upgrade\ps1-policy` directory. |
| `OAM_PS1_CONFIG_FILE_LOC` | This property refers to the Oracle Access Manager 11.1.1.5.0 configuration files available in the following location:<br>On UNIX, it is located in the `$<DOMAIN_HOME>/config/fmwconfig/oam-config.xml` directory.<br>On Windows, it is located in the `<DOMAIN_HOME>\config\fmwconfig\oam-config.xml` directory. |

*Table 4–4 (Cont.) Property Description*

| Properties | Description |
|---|---|
| `OAM_PS1_POLICY_FILE_TEMP` | This property refers to the absolute path to the temporary policy XML. This temporary XML will be used for policy transformation.<br>Specify the temporary location of the XML file.<br>For example:<br>On UNIX, specify the following path:<br>`OAM_PS1_POLICY_FILE_TEMP=<UPGRADE_ATRIFACTS_DIR>/oam-policy-ps1_temp.xml`<br>On Windows, specify the following path:<br>`OAM_PS1_POLICY_FILE_TEMP=<UPGRADE_ATRIFACTS_DIR>\oam-policy-ps1_temp.xml` |
| `OAM_R2_POLICY_JARS` | Upgrade frameworks loads version specific jars for exporting and importing data. This property refers to the Access Manager 11.1.2 policy jars available at the following location:<br>On UNIX, it is located in the `$<ORACLE_HOME>/oam/server/lib/upgrade/ps2-policy` directory.<br>On Windows, it is located in the `<ORACLE_HOME>\oam\server\lib\upgrade\ps2-policy` directory. |
| `OAM_R2_CONFIG_FILE_LOC` | This property refers to the Access Manager 11.1.2 configuration files available at the following location:<br>On UNIX, it is located in the `$<ORACLE_HOME>/oam/server/config/oam-config.xml` directory.<br>On Windows, it is located in the `<ORACLE_HOME>\oam\server\config\oam-config.xml` directory. |
| `OAM_SOURCE_VERSION` | The Oracle Access Manager source version is 11.1.1.5.0. |
| `OAM_TARGET_VERSION` | The Access Manager target version is 11.1.2. |

**Note:** The variables listed in Table 4–4 are not environment variables. These variables must be defined in the `oam_upgrade.properties` file.

### Sample Output of exportAccessData

```
wls:/offline> exportAccessData("<IAM_HOME>/oam/server/wlst/scripts/sample_
properties/oam_upgrade.properties")
Jul 7, 2012 1:37:30 AM oracle.security.access.upgrade.WLSTExecutor executeCommand
INFO: EXPORT_DATA_COMMAND
Jul 7, 2012 1:37:30 AM oracle.security.access.upgrade.util.WLSTExportDataUtil
executeCommand
INFO: OAAM PRODUCT
Jul 7, 2012 1:37:30 AM oracle.security.access.upgrade.util.WLSTExportDataUtil
executeCommand
INFO: OAM PRODUCT
Jul 7, 2012 1:37:30 AM oracle.security.access.upgrade.util.WLSTExportDataUtil
executeCommand
INFO: oamPlugin.getName() =
oracle.security.am.upgrade.plugin.upgradehelper.UpgradeFactory
Jul 7, 2012 1:37:30 AM oracle.security.am.upgrade.plugin.util.UpgradeUtil
exportConfiguration
INFO: Copying configuration file....
oracle.security.am.upgrade.plugin.upgradehelper.OAMVersionSpecificClassLoader@1e33
```

```
0f43
[EL Info]: 2012-07-07 01:37:32.849--ServerSession(503497062)--EclipseLink,
version: Eclipse Persistence Services - 1.1.0.r3634
[EL Info]: 2012-07-07 01:37:35.212--ServerSession(503497062)--file:$ORACLE_
HOME/oam/server/lib/upgrade/ps1-policy/oes-d8/jps-internal.jar-JpsDBDataManager
login successful
Jul 7, 2012 1:37:39 AM com.tangosol.coherence.component.util.logOutput.Jdk log
INFO: 2012-07-07 01:37:39.026/135.466 Oracle Coherence 3.5.3/465p2 <Info>
(thread=Main Thread, member=n/a): Loaded operational configuration from resource
"jar:file:$ORACLE_
HOME/oam/server/lib/upgrade/ps1-policy/coherence.jar!/tangosol-coherence.xml"
Jul 7, 2012 1:37:39 AM com.tangosol.coherence.component.util.logOutput.Jdk log
INFO: 2012-07-07 01:37:39.035/135.474 Oracle Coherence 3.5.3/465p2 <Info>
(thread=Main Thread, member=n/a): Loaded operational overrides from resource
"jar:file:$ORACLE_
HOME/oam/server/lib/upgrade/ps1-policy/coherence.jar!/tangosol-coherence-override-
dev.xml"
..................
WARNING: Cannot load audit configuration.
Jul 7, 2012 1:37:47 AM oracle.security.am.common.audit.AuditHandler getAuditor
WARNING: Cannot load audit configuration.
Jul 7, 2012 1:37:47 AM oracle.security.am.common.audit.AuditHandler getAuditor
WARNING: Cannot load audit configuration.
Jul 7, 2012 1:37:47 AM
oracle.security.am.upgrade.plugin.upgradehelper.UpgradeFactory exportData
INFO: Extraction Done!!
Jul 7, 2012 1:37:47 AM oracle.security.am.upgrade.plugin.util.UpgradeCommonUtil
removeDirectory
INFO: Deletion of Directory: true path: $OAM_ARTIFACTS_DIRECTORTY/temp.zip
Jul 7, 2012 1:37:47 AM
oracle.security.am.upgrade.plugin.upgradehelper.UpgradeFactory exportData
INFO: Export completed successfully!
```

## 4.11 Importing Access Data

It is necessary to import the extracted Oracle Access Manager 11.1.1.5.0 data to the Access Manager 11.1.2 schema. The Oracle Access Manager 11.1.1.5.0 domain configuration is also merged with the Access Manager 11.1.2 configuration.

To import Oracle Access Manager 11.1.1.5.0 configuration data into Access Manager 11.1.2, complete the following steps:

**On UNIX:**

1. Move from your present working directory to the `<IAM_HOME>/common/bin` directory by running the following command on the command line:

   ```
   cd <IAM_HOME>/common/bin
   ```

2. Run the following command to launch the WebLogic Scripting Tool (WLST):

   ```
   ./wlst.sh
   ```

3. At the WLST prompt, run the following script:

   ```
   importAccessData("<UPGRADE_PROPERTIES_FILE>")
   ```

   For example:

   ```
   importAccessData("<IAM_HOME>/oam/server/wlst/scripts/sample_
   properties/oam_upgrade.properties")
   ```

See Table 4–4 for sample properties and description.

4. Exit the WLST console using the `exit()` command.

### On Windows:

1. Move from your present working directory to the `<IAM_HOME>\common\bin` directory by running the following command on the command line:

   ```
   cd <IAM_HOME>\common\bin
   ```

2. Run the following command to launch the WebLogic Scripting Tool (WLST):

   ```
   wlst.cmd
   ```

3. At the WLST prompt, run the following script:

   ```
   importAccessData("<UPGRADE_PROPERTIES_FILE>")
   ```

   For example:

   ```
   importAccessData("<IAM_HOME>\\oam\\server\\wlst\\scripts\\sample_
   properties\\oam_upgrade.properties")
   ```

   See Table 4–4 for sample properties and description.

4. Exit the WLST console using the `exit()` command.

Table 4–5 describes the parameters you need to specify on the command line:

***Table 4–5 Parameters for Importing Data***

| Parameter | Description |
|---|---|
| `properties_location` | Specify the path to the `oam_upgrade.properties` file in the Oracle Access Manager 11.1.1.5.0 installation. The following example shows the complete path:<br>On UNIX, it is located in the `IDM_HOME/oam/server/wlst/scripts/sample_properties/oam_upgrade.properties` directory.<br>On Windows, it is located in the `IDM_HOME\oam\server\wlst\scripts\sample_properties\oam_upgrade.properties` directory. |

### Sample Output of importAccessData

```
wls:/offline> importAccessData("<IAM_HOME>/oam/server/wlst/scripts/sample_
properties/oam_upgrade.properties")
LOGGER intialised java.util.logging.Logger@1e26e4b1
Jul 7, 2012 1:38:25 AM oracle.security.access.upgrade.WLSTExecutor executeCommand
INFO: IMPORT_DATA_COMMAND
Jul 7, 2012 1:38:25 AM oracle.security.access.upgrade.util.WLSTImportDataUtil
executeCommand
INFO: OAAM PRODUCT IMPORT DATA
Jul 7, 2012 1:38:25 AM oracle.security.access.upgrade.util.WLSTImportDataUtil
executeCommand
INFO: OAM PRODUCT
Jul 7, 2012 1:38:25 AM oracle.security.access.upgrade.util.WLSTImportDataUtil
executeCommand
INFO: oamPlugin.getName() =
oracle.security.am.upgrade.plugin.upgradehelper.UpgradeFactory
Jul 7, 2012 1:38:27 AM
oracle.security.am.common.policy.admin.provider.xml.XMLStore <init>
INFO: Loading policy store file: $OAM_ARTIFACTS_DIRECTORTY/oam-policy.xml.
Jul 7, 2012 1:38:30 AM com.tangosol.coherence.component.util.logOutput.Jdk log
```

```
INFO: 2012-07-07 01:38:30.069/17.816 Oracle Coherence 3.7.1.1 <Info> (thread=Main
Thread, member=n/a): Loaded operational configuration from "jar:file:$MIDDLEWARE_
HOMEoracle_common/modules/oracle.coherence/coherence.jar!/tangosol-coherence.xml"
Jul 7, 2012 1:38:30 AM com.tangosol.coherence.component.util.logOutput.Jdk log
INFO: 2012-07-07 01:38:30.103/17.850 Oracle Coherence 3.7.1.1 <Info> (thread=Main
Thread, member=n/a): Loaded operational overrides from "jar:file:$MIDDLEWARE_
HOMEoracle_
common/modules/oracle.coherence/coherence.jar!/tangosol-coherence-override-dev.xml
"
Jul 7, 2012 1:38:30 AM com.tangosol.coherence.component.util.logOutput.Jdk log
INFO: 2012-07-07 01:38:30.107/17.854 Oracle Coherence 3.7.1.1 <Info> (thread=Main
Thread, member=n/a): Loaded operational overrides from "jar:file:$ORACLE_
HOME/oam/server/lib/upgrade/ps2-policy/mapstore-coherence.jar!/tangosol-coherence-
override.xml"
.....
Jul 7, 2012 1:38:36 AM oracle.security.am.common.audit.AuditHandler getAuditor
WARNING: Cannot load audit configuration.
Jul 7, 2012 1:38:36 AM oracle.security.am.common.audit.AuditHandler getAuditor
WARNING: Cannot load audit configuration.
Jul 7, 2012 1:38:36 AM oracle.security.am.common.audit.AuditHandler getAuditor
WARNING: Cannot load audit configuration.
Jul 7, 2012 1:38:38 AM
oracle.security.am.upgrade.plugin.upgradehelper.UpgradeFactory importData
INFO: Import completed successfully!!
```

## 4.12 Starting the Administration Server and Access Manager Managed Servers

**Note:** When you start the Administration Server and the Managed Servers, the Access Manager Administration console application and the Access Manager Managed server application does not start up. This is expected.

The `redeploy` command is an online WLST command. Therefore, you must start the Oracle Access Management Access Manager Administration and Managed Servers before running the `redeploy` command.

### Starting the Administration Server

To start the Administration Server, do the following:

**On UNIX**:

Run the following command:

```
cd <MW_HOME>/user_projects/domains/<domain_name>/bin
```

```
./startWebLogic.sh
```

**On Windows**:

Run the following command:

```
cd <MW_HOME>\user_projects\domains\<domain_name>\bin
```

```
startWebLogic.cmd
```

### Exceptions:

The following exception is displayed when you start the Administration Server. Ignore it:

```
<Month Date, year Time Timezone> <Error> <Deployer> <BEA-149205> <Failed to
initialize the application 'oracle.oaam.libs
[LibSpecVersion=11.1.1.3.0,LibImplVersion=11.1.1.3.0]' due to error
weblogic.application.library.LibraryDeployment
Exception: [J2EE:160145]Failed to deploy library Extension-Name: oracle.oaam.libs,
Specification-Version:11.1.2, Implementation-Version: 11.1.2.0.0, because of
conflicting library Manifest values,and library information registered with the
server:
[Specification-Version: 11.1.2 vs. 11.1.1.3, Implementation-Version:
11.1.2.0.0 vs. 11.1.1.3.0]. Check the library"s MANIFEST.MF file, and correct
version info there to match server settings. Or undeploy the misconfigured
library..
weblogic.application.library.LibraryDeploymentException: [J2EE:160145]Failed to
deploy library Extension-Name: oracle.oaam.libs, Specification-Version:
11.1.2, Implementation-Version: 11.1.2.0.0, because of conflicting library
Manifest values, and library information registered with the server:
[Specification-Version: 11.1.2 vs. 11.1.1.3, Implementation-Version:
11.1.2.0.0 vs. 11.1.1.3.0]. Check the library"s MANIFEST.MF file, and correct
version info there to match server settings. Or undeploy the misconfigured
library.
at weblogic.application.internal.library.LibraryDeploymentFactory.getLibData(Libr
aryDeploymentFactory.java:113)
at weblogic.application.internal.library.LibraryDeploymentFactory.createDeploymen
t(LibraryDeploymentFactory.java:48)
at weblogic.application.internal.DeploymentManagerImpl.createDeployment(Deploymen
tManagerImpl.java:84)
at weblogic.deploy.internal.targetserver.BasicDeployment.createDeployment(BasicDe
ployment.java:149)
at weblogic.deploy.internal.targetserver.AppDeployment.prepare(AppDeployment.java
:114)
Truncated. see log file for complete stacktrace

<Month Date, year Time Timezone> <Error> <Deployer> <BEA-149205> <Failed to
initialize the application 'oam_server' due to error
weblogic.management.DeploymentException: [Deployer:149268]Static deployment of
non-versioned application 'oam_server' failed due it its manifest defines
version..
weblogic.management.DeploymentException: [Deployer:149268]Static deployment of
non-versioned application 'oam_server' failed due it its manifest defines version.
at weblogic.deploy.internal.targetserver.AppDeployment.staticDeployValidationForN
onVersion(AppDeployment.java:186)
at
weblogic.deploy.internal.targetserver.AppDeployment.prepare(AppDeployment.java:108
)
at
weblogic.management.deploy.internal.DeploymentAdapter$1.doPrepare(DeploymentAdapte
r.java:40)
at
weblogic.management.deploy.internal.DeploymentAdapter.prepare(DeploymentAdapter.ja
va:191)
at weblogic.management.deploy.internal.AppTransit
```

### Starting Managed Servers

To start the Access Manager Managed Servers, do the following:

**On UNIX**:

1. Move from your present working directory to the `<MW_HOME>/user_projects/domains/<domain_name>/bin` directory by running the following command on the command line:

   ```
   cd <MW_HOME>/user_projects/domains/<domain_name>/bin
   ```

2. Run the following command to start the Servers:

   ```
   ./startManagedWebLogic.sh <managed_server_name> <admin_url> <user_name>
   <password>
   ```

   where

   `<managed_server_name>` is the name of the Managed Server

   `<admin_url>` is URL of the administration console. Specify it in the format `http://<host>:<port>/console`. Specify only if the WebLogic Administration Server is on a different computer.

   `<user_name>` is the username of the WebLogic Administration Server.

   `<password>` is the password of the WebLogic Administration Server.

**On Windows**:

1. Move from your present working directory to the `<MW_HOME>\user_projects\domains\<domain_name>\bin` directory by running the following command on the command line:

   ```
   cd <MW_HOME>\user_projects\domains\<domain_name>\bin
   ```

2. Run the following command to start the Managed Servers:

   ```
   startManagedWebLogic.cmd <managed_server_name> <admin_url> <user_name>
   <password>
   ```

   where

   `<managed_server_name>` is the name of the Managed Server.

   `<admin_url>` is URL of the administration console. Specify it in the format `http://<host>:<port>/console`. Specify only if the WebLogic Administration Server is on a different computer.

   `<user_name>` is the username of the WebLogic Administration Server.

   `<password>` is the password of the WebLogic Administration Server.

### Exceptions:

The following exception is displayed when you start the Managed Server. Ignore it:

```
<Month Date, year Time Timezone> <Error> <Deployer> <BEA-149205> <Failed to
initialize the application 'oracle.oaam.libs
[LibSpecVersion=11.1.1.3.0,LibImplVersion=11.1.1.3.0]' due to error
weblogic.application.library.LibraryDeploymentException: [J2EE:160145]Failed to
deploy library Extension-Name: oracle.oaam.libs, Specification-Version:
11.1.2, Implementation-Version: 11.1.2.0.0, because of conflicting library
Manifest values, and library information registered with the server:
[Specification-Version: 11.1.2 vs. 11.1.1.3, Implementation-Version:
11.1.2.0.0 vs. 11.1.1.3.0]. Check the library"s MANIFEST.MF file, and correct
version info there to match server settings. Or undeploy the misconfigured
library..
weblogic.application.library.LibraryDeploymentException: [J2EE:160145]Failed to
deploy library Extension-Name: oracle.oaam.libs, Specification-Version:
11.1.2, Implementation-Version: 11.1.2.0.0, because of conflicting library
Manifest values, and library information registered with the server:
```

```
[Specification-Version: 11.1.2 vs. 11.1.1.3, Implementation-Version:
11.1.2.0.0 vs. 11.1.1.3.0]. Check the library"s MANIFEST.MF file, and correct
version info there to match server settings. Or undeploy the misconfigured
library.
at
weblogic.application.internal.library.LibraryDeploymentFactory.getLibData(LibraryD
eploymentFactory.java:113)
at
weblogic.application.internal.library.LibraryDeploymentFactory.createDeployment(Li
braryDeploymentFactory.java:48)
at
weblogic.application.internal.DeploymentManagerImpl.createDeployment(DeploymentMan
agerImpl.java:84)
at
weblogic.deploy.internal.targetserver.BasicDeployment.createDeployment(BasicDeploy
ment.java:149)
at
weblogic.deploy.internal.targetserver.AppDeployment.prepare(AppDeployment.java:114
)
Truncated. see log file for complete stacktrace

<Month Date, year Time Timezone> <Error> <Deployer> <BEA-149205> <Failed to
initialize the application 'oam_server' due to error
weblogic.management.DeploymentException: [Deployer:149268]Static deployment
of non-versioned application 'oam_server' failed due it its manifest defines
version..
weblogic.management.DeploymentException: [Deployer:149268]Static deployment of
non-versioned application 'oam_server' failed due it its manifest defines version.
at weblogic.deploy.internal.targetserver.AppDeployment.staticDeployValidationForN
onVersion(AppDeployment.java:186)
at
weblogic.deploy.internal.targetserver.AppDeployment.prepare(AppDeployment.java:108
)
at
weblogic.management.deploy.internal.DeploymentAdapter$1.doPrepare(DeploymentAdapte
r.java:40)
at
weblogic.management.deploy.internal.DeploymentAdapter.prepare(DeploymentAdapter.ja
va:191)
at weblogic.management.deploy.internal.AppTransit
```

For more information, see "Starting the Stack" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

## 4.13 Redeploying Oracle Access Management Access Manager Servers and Shared Libraries

You must redeploy Oracle Access Management Access Manager for the following reasons:

- To uptake new shared libraries that Access Manager servers are dependent on.
- To uptake newer versions of Access Manager Administration and Managed Server applications.

To redeploy Access Manager servers and shared Access Manager libraries, complete the following steps:

**On UNIX:**

1. Move from your present working directory to the `<IAM_HOME>/common/bin` directory by running the following command on the command line:

   ```
   cd <IAM_HOME>/common/bin
   ```

2. Run the following command to launch the WebLogic Scripting Tool (WLST):

   ```
   ./wlst.sh
   ```

3. Connect to the Administration Server using the following command:

   ```
   connect('weblogic-username','weblogic-password','<weblogic_
   host>:<port>')
   ```

4. Run the following command:

   ```
   redeployOAM("<ORACLE_HOME>","<ORACLE_COMMON_HOME>",adminTarget="Admin_
   name",serverTarget="oam_server1")
   ```

   **Note:** The following exception is displayed after the Access Manager server deployment because `tmp` and `stage` directories still exists. You can ignore the errors:

   ```
   [HTTP:101216]Servlet: "AMInitServlet" failed to preload on startup
   in Web application: "oam".
   java.lang.ExceptionInInitializerError
   at java.lang.J9VMInternals.initialize(J9VMInternals.java:222)
   at
   oracle.security.am.engines.sso.adapter.AbstractSessionAdapterImpl.c
   heckAndInit(AbstractSessionAdapterImpl.java:97)
   at
   oracle.security.am.engines.sso.adapter.AbstractSessionAdapterImpl.<
   init>(AbstractSessionAdapterImpl.java:75)
   at
   oracle.security.am.engines.sso.adapter.MultipleUserSessionAdapterIm
   pl.<init>(MultipleUserSessionAdapterImpl.java:56
   at
   oracle.security.am.engines.sso.adapter.MultipleUserSessionAdapterIm
   pl.<clinit>(MultipleUserSessionAdapterImpl.java:45)
   at java.lang.J9VMInternals.initializeImpl(Native Method)
   at java.lang.J9VMInternals.initialize(J9VMInternals.java:200)
   at
   oracle.security.am.engines.sso.adapter.SessionManagementAdapterFact
   ory.getAdapter(SessionManagementAdapterFactory.java:46
   Caused by:
   oracle.security.am.common.utilities.exception.AmRuntimeException:OA
   M Server Key initialization failed
   Caused by: javax.crypto.BadPaddingException: Given final block not
   properly padded
   ```

5. Exit the WLST console using the `exit()` command.

**On Windows:**

1. Move from your present working directory to the `<IAM_HOME>\common\bin` directory by running the following command on the command line:

   ```
   cd <IAM_HOME>\common\bin
   ```

2. Run the following command to launch the WebLogic Scripting Tool (WLST):

```
wlst.cmd
```

3. Connect to the Administration Server using the following command:

```
connect('weblogic-username','weblogic-password','<weblogic_
host>:<port>')
```

4. Run the following command:

```
redeployOAM("<MW_HOME>","<ORACLE_COMMON_
HOME>",adminTarget="AdminServer",serverTarget="oam_server1"
```

**Note:** The following exception is displayed after Access Manager server deployment because the `tmp` and `stage` directories still exists. You can ignore the errors:

```
[HTTP:101216]Servlet: "AMInitServlet" failed to preload on startup
in Web application: "oam".
java.lang.ExceptionInInitializerError
at java.lang.J9VMInternals.initialize(J9VMInternals.java:222)
at
oracle.security.am.engines.sso.adapter.AbstractSessionAdapterImpl.c
heckAndInit(AbstractSessionAdapterImpl.java:97)
at
oracle.security.am.engines.sso.adapter.AbstractSessionAdapterImpl.<
init>(AbstractSessionAdapterImpl.java:75)
at
oracle.security.am.engines.sso.adapter.MultipleUserSessionAdapterIm
pl.<init>(MultipleUserSessionAdapterImpl.java:56
at
oracle.security.am.engines.sso.adapter.MultipleUserSessionAdapterIm
pl.<clinit>(MultipleUserSessionAdapterImpl.java:45)
at java.lang.J9VMInternals.initializeImpl(Native Method)
at java.lang.J9VMInternals.initialize(J9VMInternals.java:200)
at
oracle.security.am.engines.sso.adapter.SessionManagementAdapterFact
ory.getAdapter(SessionManagementAdapterFactory.java:46)
Caused by:
oracle.security.am.common.utilities.exception.AmRuntimeException:OA
M  Server Key initialization failed
Caused by: javax.crypto.BadPaddingException: Given final block not
properly padded
```

5. Exit the WLST console using the `exit()` command.

Table 4–6 describes the parameters you need to specify on the command line:

*Table 4–6 Parameters for Redeploying Access Manager Servers and Shared Libraries*

| Parameter | Description |
|---|---|
| ORACLE_HOME | Specify the complete path to the Oracle Home.<br>For example:<br>On UNIX, it is located in the `Oracle/Middleware` directory.<br>On Windows, it is located in the `Oracle\Middleware` directory. |

*Table 4–6 (Cont.) Parameters for Redeploying Access Manager Servers and Shared*

| Parameter | Description |
|---|---|
| `ORACLE_COMMON_HOME` | Specify the complete path to the Oracle common home.<br>For example:<br>On UNIX, it is located in the `Oracle/Middleware/Common_home` directory.<br>On Windows, it is located in the `Oracle\Middleware\Common_home` directory. |
| `adminTarget` | Specify the Administration Server name you have given while configuring Access Manager. |
| `serverTarget` | Specify the Managed Server name you have given while configuring Access Manager. |

The deployment may fail if the SDP library is already installed as a part of the SOA deployments. See Section 4.18.2, "Redeploy Oracle Access Management Access Manager" for recovery procedures.

## 4.14 Stopping the Administration Server and Access Manager Managed Servers

To stop the servers, see Section 4.2, "Shutting Down Administration Server and Managed Servers".

## 4.15 Deleting Folders

This step is required to uptake new version of the Access Manager Managed Server. The `redeploy` command does not delete the `tmp` directories.

In order to deploy Oracle Access Manager 11.1.1.5.0 server content and applications to Access Manager 11.1.2, you must delete all folders in the following location:

**On UNIX:**

```
<MW_Home>/user_projects/domains/domain_home/servers/<OAM_MANAGED_SERVER_
NAME>
```

**On Windows:**

```
<MW_Home>\user_projects\domains\domain_home\servers\<OAM_MANAGED_SERVER_
NAME>
```

## 4.16 Starting the Administration Server and Access Manager Managed Servers

To start the servers, see Section 4.12, "Starting the Administration Server and Access Manager Managed Servers".

**Note:** The Administration server start-up takes approximately 30 minutes due to policy migration.

## 4.17 Verifying the Upgrade

Use the following URL in a web browser to verify that Oracle Access Management Access Manager 11*g* Release 2 (11.1.2) is running:

```
http(s)://<oam_admin_server_host>:<oam_admin_server_port>/oamconsole
```

> **Note:** This note is applicable only to users who currently have Oracle Identity Manager and Oracle Access Manager components integrated in 11*g* R1 (11.1.1.5.1) or earlier versions, and are upgrading both Oracle Identity Manager and Access Manager to 11*g* R2 (11.1.2).
>
> After upgrading the components to 11*g* Release 2 (11.1.2), see "Using the idmConfigTool Command" in the *Oracle Fusion Middleware Integration Guide for Oracle Identity Management Suite*.

## 4.18 Troubleshooting

For troubleshooting topics, see the following sections:

- Section 4.18.1, "ImportAccessData"
- Section 4.18.2, "Redeploy Oracle Access Management Access Manager"
- Section 4.18.3, "Restarting Administration Server"
- Section 4.18.4, "Restarting Managed Server"

### 4.18.1 ImportAccessData

If you get a `class not found` exception, it is because you have not exited from the WLST console after running the `exportAccessData` command.

Exit the WLST console using the `exit()` command.

### 4.18.2 Redeploy Oracle Access Management Access Manager

- If you get the following exception, then the SDP library is already installed.

```
<Month <Date>, Year Time Time ZOne> <Info> <J2EE Deployment SPI> <BEA-260121>
<Initiating deploy operation for application, oracle.sdp.client#11.1.1@11.1.1
[archive: <ORACLE_HOME>/communications/modules/oracle.sdp.client_
11.1.1/sdpclient.jar], to oam_server1 .>
weblogic.management.ManagementException: [Deployer:149007]New source location,
'<ORACLE_HOME>/communications/modules/oracle.sdp.client_11.1.1/sdpclient.jar',
cannot be deployed to configured application, 'oracle.sdp.client
[LibSpecVersion=11.1.1,LibImplVersion=11.1.1]'. The application source is at
'<ORACLE_SOA_HOME>/communications/modules/oracle.sdp.client_
11.1.1/sdpclient.jar'. Changing the source location is not allowed for a
previously attempted deployment. Try deploying without specifying the
source.Failed to deploy the application with status failed
Current Status of your Deployment:
Deployment command type: deploy
Deployment State : failed
Deployment Message : weblogic.management.ManagementException:
[Deployer:149007]New source location, '<ORACLE_
HOME>/communications/modules/oracle.sdp.client_11.1.1/sdpclient.jar', cannot be
deployed to configured application, 'oracle.sdp.client
[LibSpecVersion=11.1.1,LibImplVersion=11.1.1]'. The application source is at
'<ORACLE_SOA_HOME>/communications/modules/oracle.sdp.client_
```

```
11.1.1/sdpclient.jar'. Changing the source location is not allowed for a
previously attempted deployment. Try deploying without specifying the source.
Error occured while performing deploy : Target exception thrown while deploying
application: Error occured while performing deploy : Deployment Failed. : Error
occured while performing deploy : Deployment Failed.
Use dumpStack() to view the full stacktrace
Deploying application from <ORACLE_HOME>/oam/server/apps/oam-admin.ear to
targets AdminServer (upload=false) ...
```

Complete the following steps to recover:

1. Log into the WebLogic console.
2. Check for the following library:

   **oracle.sdp.client(11.1.1,11.1.1)**
3. Target this library to `oam_server1`
4. Run the following command:

   ```
   deployOAMServer("<ORACLE_
   HOME>",adminTarget="AdminServer",serverTarget="oam_server1")
   ```

- If you get the following error after the Access Manager server deployment, it is because the `tmp` and `stage` directories still exist in your environment.

  Ignore it:

  ```
  [HTTP:101216]Servlet: "AMInitServlet" failed to preload on startup in Web
  application: "oam".
  java.lang.ExceptionInInitializerError
  at java.lang.J9VMInternals.initialize(J9VMInternals.java:222)
  at
  oracle.security.am.engines.sso.adapter.AbstractSessionAdapterImpl.checkAndInit(
  AbstractSessionAdapterImpl.java:97)
  at
  oracle.security.am.engines.sso.adapter.AbstractSessionAdapterImpl.<init>(Abstra
  ctSessionAdapterImpl.java:75)
  at
  oracle.security.am.engines.sso.adapter.MultipleUserSessionAdapterImpl.<init>(Mu
  ltipleUserSessionAdapterImpl.java:56)
  at
  oracle.security.am.engines.sso.adapter.MultipleUserSessionAdapterImpl.<clinit>(
  MultipleUserSessionAdapterImpl.java:45)
  at java.lang.J9VMInternals.initializeImpl(Native Method)
  at java.lang.J9VMInternals.initialize(J9VMInternals.java:200)
  at
  oracle.security.am.engines.sso.adapter.SessionManagementAdapterFactory.getAdapt
  er(SessionManagementAdapterFactory.java:46)
  ```

### 4.18.3 Restarting Administration Server

If you get the following error, the 11.1.2 Repository Creation Utility is not new and has data.

```
oracle.security.am.common.policy.admin.impl.PolicyValidationException:
OAMSSA-06045: An object of this type named "HTTP" already exists.
at
oracle.security.am.common.policy.admin.impl.ResourceTypeManagerImpl.isValidWrite(R
esourceTypeManagerImpl.java:482)
at
oracle.security.am.common.policy.admin.impl.ResourceTypeManagerImpl.createResource
```

```
Type(ResourceTypeManagerImpl.java:165)
at
oracle.security.am.common.policy.tools.OAMPolicyStoreBootstrap.createResourceType(
OAMPolicyStoreBootstrap.java:554)
at
oracle.security.am.common.policy.tools.OAMPolicyStoreBootstrap.addOAMObjs(OAMPolic
yStoreBootstrap.java:328)
at
oracle.security.am.common.policy.tools.OAMPolicyStoreBootstrap.addPolicyObjects(OA
MPolicyStoreBootstrap.java:280)
at
oracle.security.am.common.policy.tools.OAMPolicyStoreBootstrap.bootstrap(OAMPolicy
StoreBootstrap.java:233)
at oracle.security.am.install.OAMInstaller.bootstrapOES(OAMInstaller.java:1064)
at oracle.security.am.install.OAMInstaller.bootstrapPolicy(OAMInstaller.java:1423)
at oracle.security.am.install.OAMInstaller.upgradePolicy(OAMInstaller.java:1513)
```

Check if a new Repository Creation Utility schema is created for Access Manager. Also check if the domain has been updated to use the new 11.1.2 Repository Creation Utility.

### 4.18.4 Restarting Managed Server

If you get the following error, the `tmp` and `stage` folders still exists:

```
Caused by:
com.bea.security.ParameterException: Invalid configuration: cannot locate class:
com.bea.security.ssal.micro.MicroSecurityServiceManagerWrapper
at
com.bea.security.impl.SecurityRuntimeImpl.getNewInstance(SecurityRuntimeImpl.java:
263)
at
com.bea.security.impl.SecurityRuntimeImpl.initialize(SecurityRuntimeImpl.java:313)
at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
at sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:39)
at
sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:
25)
at java.lang.reflect.Method.invoke(Method.java:597)
at com.bea.security.SecurityRuntime.initialize(SecurityRuntime.java:140)
at com.bea.security.impl.MicroSMImpl.getInstance(MicroSMImpl.java:167)
```

This error is resolved once you remove the `tmp` and `stage` folders, as instructed in Section 4.15, "Deleting Folders".

# 5 Upgrading Oracle Adaptive Access Manager 11*g* Release 1 (11.1.1.5.0) Environments

This chapter describes how to upgrade your existing Oracle Adaptive Access Manager 11*g* Release 1 (11.1.1.5.0) environment to Oracle Adaptive Access Manager 11*g* Release 2 (11.1.2).

This chapter contains the following sections:

Read the Oracle Fusion Middleware System Requirements and Specifications document to ensure that your environment meets the minimum requirements for the products you are installing or upgrading.

## 5.1 Upgrade Roadmap for Oracle Adaptive Access Manager

> **Note:** If you do not follow the exact sequence provided in this task table, your Oracle Adaptive Access Manager upgrade may not be successful.

Table 5–1 lists the steps to upgrade Oracle Adaptive Access Manager.

***Table 5–1 Upgrade Flow***

| | Task | For More Information |
|---|---|---|
| 1 | Shut down all servers. This includes both Administration Server and Managed Servers. | See, Shutting Down Administration Server and Managed Servers |
| 2 | Back up your environment. | See, Backing Up Oracle Adaptive Access Manager 11g Release 1 (11.1.1.5.0) |
| 3 | Optional - Upgrade Oracle WebLogic Server 10.3.5 to Oracle WebLogic Server 10.3.6. | See, Optional: Upgrading Oracle WebLogic Server |
| 4 | Upgrade 11.1.1.5.0 Oracle Home to 11.1.2.0.0. | See, Upgrading Oracle Adaptive Access Manager 11g Release 2 (11.1.2) |
| 5 | Upgrade MDS schema and Audit schema using Patch Set Assistant. | See, Upgrading MDS Schema and IAU Schema Using Patch Set Assistant |
| 6 | Run Oracle Fusion Middleware Repository Creation Utility (RCU) to create and load OPSS schema for Oracle Identity and Access Management products. | See, Creating Oracle Platform Security Services Schema |
| 7 | Extend your Oracle Adaptive Access Manager 11.1.1.5.0 domain with the OPSS template. | See, Extending Oracle Adaptive Access Manager 11.1.1.5.0 Component Domains with OPSS Template |
| 8 | Upgrade Oracle Platform Security Services. | See, Upgrading Oracle Platform Security Services |
| 9 | Run the `configuresecuritystore.py` script to configure policy stores. | See, Configuring OPSS Security Store |
| 10 | Upgrade the Oracle Adaptive Access Manager schemas. | See, Upgrading Oracle Adaptive Access Manager Schema |
| 11 | Start the Administration and Managed Servers. | See, Starting the Administration Server and Oracle Adaptive Access Manager Managed Servers |
| 12 | Redeploy the applications on Oracle Adaptive Access Manager 11.1.2.0.0 Servers. | See, Redeploying the Application |
| 13 | Delete the `tmp` and `stage` folders. | See, Deleting Folders |
| 14 | Restart the servers. | See, Restarting the Servers |
| 15 | Complete the post-upgrade tasks if required. | See, Post Upgrade Steps |
| 16 | Verify the Oracle Adaptive Access Manager upgrade. | See, Verifying the Upgrade |

## 5.2 Shutting Down Administration Server and Managed Servers

The upgrade process involves changes to the binaries and to the schema. Therefore, before you begin the upgrade process, you must shut down the Administration Server and Managed Servers.

To shut down the Servers, do the following:

### Stopping the Administration Server

To stop the Administration Server, do the following:

**On UNIX**:

Run the following command:

```
cd <MW_HOME>/user_projects/domains/<domain_name>/bin
```

```
./stopWebLogic.sh
```

**On Windows**:

Run the following command:

```
cd <MW_HOME>\user_projects\domains\<domain_name>\bin
```

```
stopWebLogic.cmd
```

### Stopping Managed Servers

To stop the Managed Servers, do the following:

**On UNIX**:

1. Move from your present working directory to the `<MW_HOME>/user_projects/domains/<domain_name>/bin` directory by running the following command on the command line:

   ```
   cd <MW_HOME>/user_projects/domains/<domain_name>/bin
   ```

2. Run the following command to stop the Servers:

   ```
   ./stopManagedWebLogic.sh <server_name> <admin_url> <user_name>
   <password>
   ```

   where

   `<server_name>` is the name of the Managed Server.

   `<admin_url>` is URL of the WebLogic administration console. Specify it in the format `http://<host>:<port>/console`. Specify only if the WebLogic Administration Server is on a different computer.

   `<user_name>` is the username of the WebLogic Administration Server.

   `<password>` is the password of the WebLogic Administration Server.

**On Windows**:

1. Move from your present working directory to the `<MW_HOME>\user_projects\domains\<domain_name>\bin` directory by running the following command on the command line:

   ```
   cd <MW_HOME>\user_projects\domains\<domain_name>\bin
   ```

2. Run the following command to stop the Managed Servers:

   ```
   stopManagedWebLogic.cmd <server_name> <admin_url> <username> <password>
   ```

where

`<server_name>` is the name of the Managed Server.

`<admin_url>` is URL of the WebLogic administration console. Specify it in the format `http://<host>:<port>/console`. Specify only if the WebLogic Administration Server is on a different computer.

`<username>` is the username of the WebLogic Administration Server.

`<password>` is the password of the WebLogic Administration Server.

For more information, see "Stopping the Stack" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

## 5.3 Backing Up Oracle Adaptive Access Manager 11*g* Release 1 (11.1.1.5.0)

You must back up your Oracle Adaptive Access Manager 11.1.1.5.0 environment before you upgrade to Oracle Adaptive Access Manager 11.1.2.

After stopping the servers, you must back up the following:

- *MW_HOME* directory, including the Oracle Home directories inside Middleware Home
- Domain Home directory
- Oracle Adaptive Access Manager schemas
- IAU schema, if it is part of any of your Oracle Adaptive Access Manager 11.1.1.5.0 schemas
- MDS schemas

## 5.4 Optional: Upgrading Oracle WebLogic Server

**Note:** Upgrading Oracle WebLogic Server is not mandatory. However, Oracle recommends that you upgrade Oracle WebLogic Server to 10.3.6.

You can upgrade WebLogic Server 10.3.5 to Oracle WebLogic Server 10.3.6 by using the WebLogic 10.3.6 Upgrade Installer. Complete the following steps:

1. Download the WebLogic 10.3.6 Upgrade Installer from Oracle Technology Network.

   For more information, see "Downloading the Installer From Oracle Technology Network" in the *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*.

2. Run the Upgrade Installer in graphical mode to upgrade your WebLogic Server.

   For more information, see "Running the Upgrade Installer in Graphical Mode" in the *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*.

## 5.5 Upgrading Oracle Adaptive Access Manager 11*g* Release 2 (11.1.2)

To upgrade Oracle Adaptive Access Manager, you must use the Oracle Identity and Access Management 11.1.2 Installer. During the procedure, point the Middleware Home to your existing 11.1.1.5.0 Middleware Home. Your Oracle Home is upgraded from 11.1.1.5.0 to 11.1.2.

This section contains the following topics:

- Obtaining the Software
- Starting the Oracle Identity and Access Management Installer
- Installing Oracle Identity and Access Management 11g Release 2 (11.1.2)

### 5.5.1 Obtaining the Software

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

### 5.5.2 Starting the Oracle Identity and Access Management Installer

This topic explains how to start the Oracle Identity and Access Management 11.1.2 Installer.

**Notes:**

- If you are installing 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 doing the following:

**On UNIX**:

1. Move from your present working directory to the directory where you extracted the contents of the Installer to.
2. Move to the following location:

   ```
   cd Disk1
   ```

3. Run the following command:

   ```
   ./runInstaller -jreLoc <complete path to the JRE directory>
   ```

   For example:

   ```
   ./runInstaller -jreLoc <MW_HOME>/jdk160_29/jre
   ```

**On Windows**:

1. Move from your present working directory to the directory where you extracted the contents of the Installer to.
2. Move to the following location:

   ```
   cd Disk1
   ```

3. Run the following command:

   ```
   setup.exe -jreLoc <complete path to the JRE directory>
   ```

For example:

```
setup.exe -jreLoc <MW_HOME>\jdk160_29\jre
```

> **Note:** 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 is not created in your Middleware Home. You must enter the absolute path to the JRE folder from where your JDK is located.

### 5.5.3 Installing Oracle Identity and Access Management 11*g* Release 2 (11.1.2)

Use the Oracle Adaptive Access Manager 11.1.2 Installer to upgrade Oracle Adaptive Access Manager 11.1.1.5.0 to OAAM 11.1.2:

1. After you start the installer, the **Welcome** screen appears.
2. Click **Next** on the **Welcome** screen. The **Install Software Updates** screen appears. Select whether or not you want to search for updates. Click **Next**.
3. The **Prerequisite Checks** screen appears. If all prerequisite checks pass inspection, click **Next**. The **Specify Installation Location** screen appears.
4. On the **Specify Installation Location** screen, point the Middleware Home to your existing 11.1.1.5.0 Middleware Home installed on your system.
5. In the **Oracle Home Directory** field, specify the path of the existing Oracle Identity and Access Management Home. This directory is also referred to as `<IAM_HOME>` in this book.

   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 you want to proceed with 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 **Help** on the installation wizard screens.

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

   This installation process copies the 11.1.2 Oracle Identity and Access Management software binaries to your system.

For more information, see "Installing and Configuring Oracle Identity and Access Management (11.1.2)" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

## 5.6 Upgrading MDS Schema and IAU Schema Using Patch Set Assistant

You must upgrade your MDS schema using Patch Set Assistant. You must also upgrade your Audit (IAU) schema if it is part of your 11.1.1.5.0 schemas.

This section consists of the following topics:

- Section 5.6.1, "Checking Your Database and Schemas"
- Section 5.6.2, "Starting Patch Set Assistant"
- Section 5.6.3, "Using the Patch Set Assistant Graphical Interface"
- Section 5.6.4, "Verifying Schema Upgrade"

### 5.6.1 Checking Your Database and Schemas

Before running Patch Set Assistant, you should make sure that your database is running and that the schemas are supported. To check this, run the following SQL command:

```
SELECT OWNER, VERSION, STATUS, UPGRADED FROM SCHEMA_VERSION_REGISTRY;
```

If the number in the "VERSION" column is 11.1.1.5.0, then the schema is supported for upgrade.

> **Note:** If you are using an Oracle database, you should recompile database objects before running the Patch Set Assistant by connecting to the database as SYS and running the following from SQL*Plus:
>
> ```
> @?/rdbms/admin/utlrp.sql
> ```
>
> After running `utlrp.sql`, and before you upgrade your schema, issue the following query to ensure there are no longer any invalid database objects:
>
> ```
> SELECT owner, object_name FROM all_objects WHERE
> status='INVALID';
> ```
>
> Take note of any invalid objects. The existence of invalid database objects may prevent the upgrade from completing successfully.

### 5.6.2 Starting Patch Set Assistant

To start Patch Set Assistant, do the following:

**On UNIX:**

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

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

2. Run the following command:

   ```
   ./psa
   ```

**On Windows:**

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

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

2. Execute the following command:

   ```
   psa.bat
   ```

### 5.6.3 Using the Patch Set Assistant Graphical Interface

> **Note:** Even if you upgrade your schemas from 11.1.1.5.0 to 11.1.2.0.0, you will see the Patch Set Assistant version number as 11.1.1.6.1 on the **Welcome** screen.
>
> This is not an error. The discrepancy is caused by a difference between how Patch Set Assistant and Identity Access Management releases are tracked internally.

After starting the Patch set Assistant Installer, follow the instructions on the screen to update your schemas.

Follow the instructions in Table 5–2 to update your schemas:

***Table 5–2 Patch Set Assistant Screens***

| Screen | Description |
|---|---|
| Welcome | This page introduces you to Patch Set Assistant. |
| Select Component | Select the top-level component you want to upgrade. |
| Prerequisite | Verify that you have satisfied the database prerequisites. |
| Schema | Specify your database credentials to connect to your database, then select the schema you want to update.<br>Note that this screen appears once for each schema that must be updated as a result of the component you selected on the Select Component screen. |
| Examine | This page displays the status of the Patch Set Assistant as it examines each component schema. Verify that your schemas have a "successful" indicator in the Status column. |
| Upgrade Summary | Verify that the schemas are the ones you want to upgrade. |
| Upgrade Progress | This screen shows the progress of the schema upgrade. |
| Upgrade Success | Once the upgrade is successful, you get this screen. |

### 5.6.4 Verifying Schema Upgrade

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

**On UNIX:**

```
<MW_HOME>/oracle_common/upgrade/logs/psatimestamp.log
```

**On Windows:**

```
<MW_HOME>\oracle_common\upgrade\logs\psatimestamp.log
```

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

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

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

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

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

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

## 5.7 Creating Oracle Platform Security Services Schema

You must create Oracle Platform Security Services (OPSS) schema because Oracle Adaptive Access Manager upgrade process involves OPSS schema policy store changes. Keys, roles, permissions, and other artifacts used by the applications must migrate to the policy store.

Run Repository Creation utility (RCU) to create the OPSS schema.

For more information, see "Creating Schemas" in the *Oracle Fusion Middleware Repository Creation Utility User's Guide*.

> **Note:** In the **Select Components** screen, expand **AS Common Schemas** and select **Oracle Platform Security Services**. The **Metadata Services** schema is selected automatically. Deselect it and ignore the following message:
>
> ```
> Following components require Metadata Services schema:
> Oracle Platform Security Services.
> ```

## 5.8 Extending Oracle Adaptive Access Manager 11.1.1.5.0 Component Domains with OPSS Template

Oracle Adaptive Access Manager 11.1.2 uses the database to store policies. This requires extending the 11.1.1.5.0 Oracle Adaptive Access Manager domain to include the OPSS data source.

To do so, complete the following steps:

1. Run the following command to launch the Oracle Fusion Middleware configuration wizard:

   **On UNIX:**

   ```
   ./config.sh
   ```

   It is located in the `<MW_HOME>/<Oracle_IDM1>/common/bin` directory.

   **On Windows:**

   ```
   config.cmd
   ```

It is located in the `<MW_HOME>\<Oracle_IDM1>\common\bin` directory.

2. On the **Welcome** screen, select the **Extend an existing WebLogic domain** option. Click **Next**.
3. On the **Select a WebLogic Domain Directory** screen, browse to the directory that contains the WebLogic domain in which you configured the components. Click **Next**. The **Select Extension Source** screen is displayed.
4. On the **Select Extension Source** screen, select the **Oracle Platform Security Service - 11.1.1.0 [Oracle_IDM1]** option. After selecting the domain configuration options, click **Next**.
5. The **Configure JDBC Data Sources** screen is displayed. Configure the opssDS data source, as required. After the test succeeds, the **Configure JDBC Component Schema** screen is displayed.
6. On the **Configure JDBC Component Schema** screen, select the **Oracle Platform Security Services** schema.

   You can set values for Schema Owner, Schema Password, Database and Service, Host Name, and Port. Click **Next**.

   The **Test JDBC Component Schema** screen is displayed. After the test succeeds, the **Select Optional Configuration** screen is displayed.
7. On the **Select Optional Configuration** screen, you can configure Managed Servers, Clusters, and Machines and Deployments and Services. Do not select anything as you have already configured in your Oracle Identity and Access Management 11.1.1.5.0 environment. Click **Next**.
8. On the **Configuration Summary** screen, review the domain configuration, and click **Extend** to start extending the domain.

Your existing Oracle Adaptive Access Manager domain is extended to support Oracle Platform Security Services (OPSS).

## 5.9 Upgrading Oracle Platform Security Services

To upgrade Oracle Platform Security Services (OPSS) schema, do the following:

### On UNIX:

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

   ```
   cd <MW_HOME>/oracle_common/common/bin
   ```
2. Run the following command to launch the WebLogic Scripting Tool (WLST):

   ```
   ./wlst.sh
   ```
3. At the WLST prompt, run the following command:

   ```
   upgradeOpss(jpsConfig="existing_jps_config_file", jaznData="system_
   jazn_data_file")
   ```

   For example:

   ```
   upgradeOpss(jpsConfig="<MW_HOME>/user_projects/domains/base_
   domain/config/fmwconfig/jps-config.xml",jaznData="<MW_HOME>/oracle_
   common/modules/oracle.jps_11.1.1/domain_config/system-jazn-data.xml")
   ```
4. Exit the WLST console using the `exit()`command.

**On Windows:**

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

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

2. Run the following command to launch the WebLogic Scripting Tool (WLST):

   ```
   wlst.cmd
   ```

3. At the WLST prompt, run the following command:

   ```
   upgradeOpss(jpsConfig="existing_jps_config_file", jaznData="system_
   jazn_data_file")
   ```

   For example:

   ```
   upgradeOpss(jpsConfig="<MW_HOME>\\user_projects\\domains\\base_
   domain\\config\\fmwconfig\\jps-config.xml",jaznData="<MW_HOME>\\oracle_
   common\\modules\\oracle.jps_11.1.1\\domain_
   config\\system-jazn-data.xml")
   ```

4. Exit the WLST console using the `exit()` command.

Table 5–3 describes the parameters you need to specify on the command line:

***Table 5–3 Parameters for Upgrading OPSS***

| Parameter | Description |
|---|---|
| `jpsConfig` | Specify the path to the `jps-config.xml` file in your 11.1.2 installation. The following example shows the complete path:<br>On UNIX, it is located in the `<MW_HOME>/user_projects/domains/base_domain/config/fmwconfig/jps-config.xml` directory.<br>On Windows, it is located in the `<MW_HOME>\user_projects\domains\base_domain\config\fmwconfig\jps-config.xml directory.` |
| `jaznData` | Specify the path to the system-jazn-data.xml file in your 11.1.2 installation. The following example shows the complete path:<br>On UNIX, it is located in the `<MW_HOME>/oracle_common/modules/oracle.jps_11.1.1/domain_config/system-jazn-data.xml` directory.<br>On Windows, it is located in the `<MW_HOME>\oracle_common\modules\oracle.jps_11.1.1\domain_config\system-jazn-data.xml` directory. |

## 5.10 Configuring OPSS Security Store

You must configure the database Security Store as it is the only security store type supported by Oracle Identity and Access Management 11g Release 2 (11.1.2).

For more information on configuring Oracle Platform Security Services, see "Configuring Database Security Store for an Oracle Identity and Access Management Domain" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

## 5.11 Upgrading Oracle Adaptive Access Manager Schema

To support the latest features and changes that are included in this release, you must upgrade the Oracle Adaptive Access Manager database schema to 11.1.2.0.0. This schema upgrade is done through an offline WLST command.

To upgrade the Oracle Adaptive Access Manager schema, complete the following steps:

**On UNIX:**

1. Open `access_upgrade.properties` file in a text editor from the following location:

   ```
   $<ORACLE_HOME>/common/wlst
   ```

   Update the values, as listed in Table 5–4:

2. Move from your present working directory to the `<IAM_HOME>/common/bin` directory by running the following command on the command line:

   ```
   cd <IAM_HOME>/common/bin
   ```

3. Run the following command to launch the WebLogic Scripting Tool (WLST):

   ```
   ./wlst.sh
   ```

4. Upgrade the Oracle Adaptive Access Manager 11.1.1.5.0 schemas to 11.1.2 schemas by running the following command:

   ```
   upgradeAccessSchema(filePath="access_upgrade.properties_Location")
   ```

   where

   `filepath` is the complete the path to the `access_upgrade.properties` file in the Oracle Adaptive Access Manager installation.

   For example:

   ```
   upgradeAccessSchema(filePath="<MW_HOME>/<Oracle_
   IDM1>/common/wlst/access_upgrade.properties")
   ```

5. The `OAAM_DB_SYS_PASSWORD` is prompted. Enter the SYS password.

**On Windows:**

1. Open `access_upgrade.properties` file in a text editor from the following location:

   ```
   <ORACLE_HOME>\common\wlst
   ```

   Update the values, as listed in Table 5–4:

2. Move from your present working directory to the `<IAM_HOME>\common\bin` directory by running the following command on the command line:

   ```
   <IAM_HOME>\common\bin
   ```

3. Run the following command to launch the WebLogic Scripting Tool (WLST):

   ```
   wlst.cmd
   ```

4. Upgrade the Oracle Adaptive Access Manager 11.1.1.5.0 schemas to 11.1.2 schemas by running the following command:

   ```
   upgradeAccessSchema(filePath="access_upgrade.properties_Location")
   ```

   where

   `filepath` is the complete the path to the `access_upgrade.properties` file in the Oracle Adaptive Access Manager installation.

For example:

```
upgradeAccessSchema(filePath="<MW_HOME>\\<Oracle_
IDM1>\\common\\wlst\\access_upgrade.properties")
```

5. The `OAAM_DB_SYS_PASSWORD` is prompted. Enter the SYS password.

***Table 5–4 Parameters for Updating access_upgrade.properties File***

| Parameters | Description |
|---|---|
| `OAAM_DB_SCHEMA_USERNAME` | Specify the 11g Oracle Adaptive Access Manager schema user name. |
| `OAAM_DB_URL` | The database URL format is `<hostname>:port:sid` |
| `OAAM_DB_SYS_USERNAME` | Specify SYS as SYSDBA |
| `OAAM_ORACLE_HOME` | Specify the path to the Oracle Adaptive Access Manager home. The following example shows the complete path:<br>On UNIX, it is located in the `<MW_HOME>/<IAM_HOME>` directory.<br>On Windows, it is located in the `<MW_HOME>\<IAM_HOME>` directory. |
| `OAAM_DOMAIN_HOME` | Specify the path to the domain home. The following example shows the complete path:<br>On UNIX, it is located in the `<MW_HOME>/user_projects/domains/<oaam_domain>` directory.<br>On Windows, it is located in the `<MW_HOME>\user_projects\domains\<oaam_domain>` directory. |
| `OAAM_DB_10g` | Set the value as `false`.<br>The value `true` is required only if it is an Oracle Adaptive Access Manager 10*g* to 11.1.2 schema upgrade. |

### Example parameters

**On UNIX:**

```
OAAM_DB_SCHEMA_USERNAME=EXAMPLE_OAAM
OAAM_DB_URL=db.example.com:1521:ex
OAAM_DB_SYS_USERNAME=sys as sysdba
OAAM_ORACLE_HOME=/<MW_HOME>/<IAM_HOME>
OAAM_DOMAIN_HOME=/<MW_HOME>/user_projects/domains/<DOMAIN_NAME>
OAAM_DB_10g=false
```

**On Windows:**

```
OAAM_DB_SCHEMA_USERNAME=EXAMPLE_OAAM
OAAM_DB_URL=db.example.com:1521:ex
OAAM_DB_SYS_USERNAME=sys as sysdba
OAAM_ORACLE_HOME=\<MW_HOME>\<IAM_HOME>
OAAM_DOMAIN_HOME=\<MW_HOME>\user_projects\domains\<DOMAIN_NAME>
OAAM_DB_10g=false
```

## 5.12 Starting the Administration Server and Oracle Adaptive Access Manager Managed Servers

The `redeploy` command is an online WLST command. Therefore, you must start the Oracle Adaptive Access Manager Administration and Managed Servers before running the `redeploy` command.

### Starting Administration Server

To start the Administration Server, do the following:

**On UNIX**:

Run the following command:

```
cd <MW_HOME>/user_projects/domains/<domain_name>/bin
```

```
./startWebLogic.sh
```

**On Windows**:

Run the following command:

```
cd <MW_HOME>\user_projects\domains\<domain_name>\bin
```

```
startWebLogic.cmd
```

### Starting Managed Servers

To start the Managed Servers, do the following:

**On UNIX**:

1. Move from your present working directory to the `<MW_HOME>/user_projects/domains/<domain_name>/bin` directory by running the following command on the command line:

   ```
   cd <MW_HOME>/user_projects/domains/<domain_name>/bin
   ```

2. Run the following command to start the Servers:

   ```
   ./startManagedWebLogic.sh <managed_server_name> <admin_url> <user_name>
   <password>
   ```

   where

   `<managed_server_name>` is the name of the Managed Server

   `<admin_url>` is URL of the WebLogic administration console. Specify it in the format `http://<host>:<port>/console`. Specify only if the WebLogic Administration Server is on a different computer.

   `<user_name>` is the username of the WebLogic Administration Server.

   `<password>` is the password of the WebLogic Administration Server.

**On Windows**:

1. Move from your present working directory to the `<MW_HOME>\user_projects\domains\<domain_name>\bin` directory by running the following command on the command line:

   ```
   cd <MW_HOME>\user_projects\domains\<domain_name>\bin\
   ```

2. Run the following command to start the Managed Servers:

   ```
   startManagedWebLogic.cmd <managed_server_name> <admin_url> <user_name>
   <password>
   ```

   where

   `<managed_server_name>` is the name of the Managed Server.

   `<admin_url>` is URL of the administration console. Specify it in the format `http://<host>:<port>/console`. Specify only if the WebLogic Administration Server is on a different computer.

`<user_name>` is the username of the WebLogic Administration Server.

`<password>` is the password of the WebLogic Administration Server.

For more information, see "Starting the Stack" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

## 5.13 Redeploying the Application

You must redeploy changes to the application in the domain after upgrading. Redeploy your 11.1.1.5.0 application on the Oracle Adaptive Access Manager 11.1.2 servers.

To redeploy, complete the following steps:

**On UNIX:**

1. Move from your present working directory to the `<IAM_HOME>/common/bin` directory by running the following command on the command line:

   ```
   cd <IAM_HOME>/common/bin
   ```

2. Run the following command to launch the WebLogic Scripting Tool (WLST):

   ```
   ./wlst.sh
   ```

3. Connect to the Administration Server using the following command:

   ```
   connect('weblogic-username','weblogic-password','weblogic-url')
   ```

4. At the WLST prompt, run the following WLST command:

   ```
   redeployApps($<ORACLE_HOME>,adminTarget='<oaam_admin_
   server1>',serverTarget='<oaam_server_server1>')
   ```

   Where

   `<oaam_server_server1>` is the Managed Server on which the Oracle Adaptive Access Manager server application is deployed.

   > **Note:** Include offline Target, if Oracle Adaptive Access Manager Offline Server is present in your setup.

5. Exit the WLST console using the `exit()` command.

**On Windows:**

1. Move from your present working directory to the `<IAM_HOME>\common\bin` directory by running the following command on the command line:

   ```
   cd <IAM_HOME>\common\bin
   ```

2. Run the following command:

   ```
   wlst.cmd
   ```

3. Connect to the Administration Server using the following command:

   ```
   connect('weblogic-username','weblogic-password','weblogic-url')
   ```

4. At the WLST prompt, run the following WLST command:

   ```
   redeployApps(<MW_HOME>\\<IAM_HOME>,adminTarget='<oaam_admin_
   server1>',serverTarget='<oaam_server_server1>')
   ```

Where

`<oaam_server_server1>` is the Managed Server on which the Oracle Adaptive Access Manager server application is deployed.

> **Note:** Include offlineTarget, if Oracle Adaptive Access Manager Offline Server is present in your setup.

5. Exit the WLST console using the `exit()` command.

## 5.14 Deleting Folders

To deploy Oracle Adaptive Access Manager 11.1.1.5.0 server content and applications in Oracle Adaptive Access Manager 11.1.2, you must delete all content of folders in the following locations:

**On UNIX:**

Deleting tmp:

```
<MW_Home>/user_projects/domains/domain_home/servers/<OAAM_ADMIN_SERVER_
NAME>/tmp
```

```
<MW_Home>/user_projects/domains/domain_home/servers/<OAAM_MANAGED_SERVER_
NAME>/tmp
```

```
<MW_Home>/user_projects/domains/domain_home/servers/<OAAM_OFFLINE_SERVER_
NAME>/tmp
```

Deleting stage:

```
<MW_Home>/user_projects/domains/domain_home/servers/<OAAM_ADMIN_SERVER_
NAME>/stage
```

```
<MW_Home>/user_projects/domains/domain_home/servers/<OAAM_MANAGED_SERVER_
NAME>/stage
```

```
<MW_Home>/user_projects/domains/domain_home/servers/<OAAM_OFFLINE_SERVER_
NAME>/stage
```

**On Windows:**

Deleting tmp:

```
<MW_Home>\user_projects\domains\domain_home\servers\<OAAM_ADMIN_SERVER_
NAME>\tmp
```

```
<MW_Home>\user_projects\domains\domain_home\servers\<OAAM_MANAGED_SERVER_
NAME>\tmp
```

```
<MW_Home>\user_projects\domains\domain_home\servers\<OAAM_OFFLINE_SERVER_
NAME>\tmp
```

Deleting stage:

```
<MW_Home>\user_projects\domains\domain_home\servers\<OAAM_ADMIN_SERVER_
NAME>\stage
```

```
<MW_Home>\user_projects\domains\domain_home\servers\<OAAM_MANAGED_SERVER_
NAME>\stage
```

```
<MW_Home>\user_projects\domains\domain_home\servers\<OAAM_OFFLINE_SERVER_
NAME>\stage
```

## 5.15 Restarting the Servers

To restart the Administration Server or Managed Servers, you must stop the running Administration Server or Managed Servers first before starting them again.

To stop the servers, see Section 5.2, "Shutting Down Administration Server and Managed Servers".

To start the servers, see Section 5.12, "Starting the Administration Server and Oracle Adaptive Access Manager Managed Servers".

## 5.16 Post Upgrade Steps

Perform the following additional post-upgrade tasks after upgrading your Oracle Adaptive Access Manager 11.1.1.5.0 environment to Oracle Adaptive Access Manager 11.1.2, if required.

### 5.16.1 Upgrading Self Registration and Self Tracking URL

**Note:** Perform the following task only if you have integrated Oracle Adaptive Access Manager with Oracle Identity Manager in 11.1.1.5.0.

Upgrade the Self Registration and Self Tracking URLs as follows:

1. Log in to the Oracle Adaptive Access Manager Administration console:

   ```
   http://oaam_managed_server_host:oaam_admin_managed_server_port/oaam_
   admin
   ```

   You must log in as a user with access to the Properties Editor.

2. Open the Oracle Adaptive Access Manager Property Editor and upgrade the following:

   - `bharosa.uio.default.signon.links.enum.selfregistration.url`: Specify the Self Registration URL.

     For example:

     ```
     http://<OIM Managed Server Host>:<OIM Managed Server
     Port>/identity/faces/register?&=backUrl=<back URL>
     ```

   - `bharosa.uio.default.signon.links.enum.trackregistration.url`: Specify the Track Registration URL.

     For example:

     ```
     http://<OIM Managed Server Host>:<OIM Managed Server
     Port>/identity/faces/trackregistration?&=backUrl=<back URL>
     ```

### 5.16.2 Upgrading Security Policies Without Erasing Old Policies

Complete the following steps to upgrade your security policies without erasing your old policies:

1. Back up all of your old policies.

2. Export the policies, policies are exported as snapshots.
3. Import base entities, if you have not done so in the earlier release.
4. Import patterns.
5. Import policies.

> **Note:** If you want to completely move to new content, back up the old content and import the new snapshot.
>
> If you want to continue using old policies with the risk involved, no action is required.

## 5.17 Verifying the Upgrade

Use the following URL in a web browser to verify that Oracle Adaptive Access Manager 11.1.2 is running:

```
http://oaam.example.com:<oaam_port>/oaam_admin
```

Assign the investigator role and verify to see the investigator UI.

# 6 Upgrading Oracle Identity Manager 11*g* Release 1 (11.1.1.5.0) Environments

This chapter describes how to upgrade your existing Oracle Identity Manager 11*g* Release 1 (11.1.1.5.0) environment to Oracle Identity Manager 11*g* Release 2 (11.1.2).

This chapter contains the following sections:

Read the Oracle Fusion Middleware System Requirements and Specifications document to ensure that your environment meets the minimum requirements for the products you are installing or upgrading.

## 6.1 Feature Comparison

Table 6–1 lists the key differences in functionality between Oracle Identity Manager 11*g* Release 1 (11.1.1.5.0) and Oracle Identity Manager 11*g* Release 2 (11.1.2).

***Table 6–1 Features Comparison***

| Oracle Identity Manager 11*g* Release 1 (11.1.1.5.0) | Oracle Identity Manager 11*g* Release 2 (11.1.2) |
|---|---|
| Separate interfaces for end-user self-service and delegated administration. | A unified interface for end user self service and delegated administration. |
| Search for access items, such as roles, entitlements, or applications through a complex set of menus. | OIM users can navigate to the OIM catalog directly, search for access items, and submit a request. They can also associate metadata with each of the access items. |
| Incomprehensible resource and IT resource names that make the access request process difficult. | Intuitive, easy-to-understand resource names through an abstraction named Application Instances, which are a combination of an IT resource instance and a resource object. |
| Manual, tedious process of creating and configuring disconnected applications. | Simplified onboarding of disconnecting applications that enables system integrators to create and manage access to disconnected applications. |

*Table 6–1 (Cont.) Features Comparison*

| Oracle Identity Manager 11*g* Release 1 (11.1.1.5.0) | Oracle Identity Manager 11*g* Release 2 (11.1.2) |
|---|---|
| Users' access controlled by request templates granted to users, based on their role membership. | A user's access controlled by a combination of end-user's publishing and the access items publishing in organizations. |
| OIM-specific user interface to administer end user "authorization policies". | Authorization Policy Manager, a standards-based UI, used to administer authorization policies. This standardized UI allows administrators to administer and manage policies across the Oracle Identity Management suite of products. |
| Evaluation of access policies for each user as soon as the user is updated. | Evaluation of access policies in a fixed set of time intervals when the Evaluate User Policies scheduled job is run. |

## 6.2 Upgrade Roadmap for Oracle Identity Manager

The procedure for upgrading Oracle Identity Manager 11.1.1.5.0 to 11.1.2 involves the following high-level steps:

1. **Pre-Upgrade Steps**: This step involves tasks like generating the pre-upgrade report, analyzing the report and performing the necessary pre-upgrade tasks described in the report, shutting down the servers, backing up the 11.1.1.5.0 environment and so on.
2. **Upgrading the Oracle Home and Database Schemas**: This step involves tasks like upgrading Oracle SOA Suite, upgrading 11.1.1.5.0 Oracle Home to 11.1.2, creating Oracle Platform Security Services schema using Repository Creation Utility, upgrading Oracle Platform Security Services, configuring the security store, upgrading Oracle Identity Manager using Patch Set Assistant and so on.
3. **Upgrading the Oracle Identity Manager Middle Tier**: This step involves tasks like upgrading Oracle Identity Manager middle tier, starting the servers, patching the Oracle Identity Manager MDS metadata and so on.
4. **Upgrading Other Oracle Identity Manager Installed Components**: This step involves tasks like upgrading Oracle Identity Manager Design Console, Oracle Identity Manager Remote Manger, and configuring BI Publisher Reports.
5. **Post-Upgrade Steps**: This step involves the post-upgrade tasks like enabling Oracle Identity Manager - Oracle Access Manager integration, upgrading user UDF, customizing event handlers, upgrading SOA composites and so on.

Table 6–2 lists the steps to upgrade Oracle Identity Manager 11.1.1.5.0.

> **Note:** If you do not follow the exact sequence provided in this task table, your Oracle Identity Manager upgrade may not be successful.

*Table 6–2 Upgrade Flow*

| SI No | Task | For More Information |
|---|---|---|
| | **Pre-Upgrade Steps** | |
| 1 | Review the changes in the features of Oracle Identity Manager 11.1.2. | See, Feature Comparison |

*Table 6–2 (Cont.) Upgrade Flow*

| Sl No | Task | For More Information |
|---|---|---|
| 2 | Generate the pre-upgrade report by running the `PreUpgradeReport` utility. | See, Generating the Pre-Upgrade Report |
| 3 | Analyze the report and complete the pre-upgrade actions described in the report. | See, Analyzing Pre-Upgrade Report |
| 4 | Empty the `oimProcessQueue` JMS queue to ensure that JMS messages are processed before you start upgrading. | See, Emptying the oimProcessQueue JMS Queue |
| 5 | Complete all of the pre-requisite tasks. | See, Other Prerequisites |
| 6 | Shut down all servers. This includes Administration Server, SOA Managed Servers, and Oracle Identity Manager Managed Servers. | See, Shutting Down Administration Server and Managed Servers |
| 7 | Back up your environment. | See, Backing Up Oracle Identity Manager 11g Release 1 (11.1.1.5.0) |
| 8 | Ensure that the JRF is upgraded. | See, Ensuring That JRF is Upgraded |
| | **Upgrading the Oracle Home and Database Schemas** | |
| 9 | Optional - Upgrade Oracle WebLogic Server 10.3.5 to Oracle WebLogic Server 10.3.6. | See, Optional: Upgrading Oracle WebLogic Server |
| 10 | Upgrade SOA suite used by Oracle Identity Manager. | See, Upgrading Oracle SOA Suite Used by Oracle Identity Manager |
| 11 | Upgrade 11.1.1.5.0 Oracle Home to 11.1.2. | See, Upgrading Oracle Identity Manager 11g Release 2 (11.1.2) |
| 12 | Run Oracle Fusion Middleware Repository Creation Utility (RCU) to create and load OPSS schema for Oracle Identity and Access Management products. | See, Creating Oracle Platform Security Services Schema |
| 13 | Extend your Oracle Identity Manager 11.1.1.5.0 domain with the OPSS template. | See, Extending Oracle Identity Manager 11.1.1.5.0 Component Domains with OPSS Template |
| 14 | Upgrade Oracle Platform Security Services. | See, Upgrading Oracle Platform Security Services |
| 15 | Run the `configuresecuritystore.py` script to configure policy stores. | See, Configuring OPSS Security Store |
| 16 | Upgrade Oracle Identity Manager using the Patch Set Assistant. | See, Upgrading Oracle Identity Management Schemas Using Patch Set Assistant |
| 17 | Start the WebLogic Administration Server. | See, Starting the Administration Server and SOA Managed Servers |
| | **Upgrading the Oracle Identity Manager Middle Tier** | |
| 18 | Set Oracle Identity Manager Environment variables. | See, Setting Environment Variables |

*Table 6–2 (Cont.) Upgrade Flow*

| SI No | Task | For More Information |
|---|---|---|
| 19 | Upgrade Oracle Identity Manager Middle Tier. | See, Upgrading Oracle Identity Manager Middle Tier |
| 20 | Verify the Oracle Identity Manager Middle Tier Upgrade. | See, Verifying Oracle Identity Manager Middle Tier Upgrade |
| 21 | Change the deployment order of Oracle Identity Manager from 47 to 48. | See, Changing the Deployment Order of Oracle Identity Manager EAR |
| 22 | Restart the Administration Server and SOA Managed Servers. | See, Restarting the Administration Server and SOA Managed Server |
| 23 | Patch the Oracle Identity Manager MDS metadata by starting the Oracle Identity Manager Managed Servers. | See, Patching Oracle Identity Management MDS Metadata |
| | **Upgrading Other Oracle Identity Manager Installed Components** | |
| 24 | Upgrade Oracle Identity Manager Design Console. | See, Upgrading Oracle Identity Manager Design Console |
| 25 | Upgrade Oracle Identity Manager Remote Manager. | See, Upgrading Oracle Identity Manager Remote Manager |
| 26 | Configure BI Publisher Reports | See, Configuring BI Publisher Reports |
| | **Post-Upgrade Steps** | |

*Table 6–2 (Cont.) Upgrade Flow*

| Sl No | Task | For More Information |
|---|---|---|
| 27 | Complete the post-upgrade steps. | Post upgrade tasks include the following:<br>■ After You Upgrade<br>■ Validating the Database Objects<br>■ Creating sysadmin Key<br>■ Impact of Removing Approver-Only Attribute in Request Data Set<br>■ Changes to Request API After Upgrading to Oracle Identity Manager 11g Release 2 (11.1.2)<br>■ Enabling Oracle Identity Manager-Oracle Access Manager Integration After Upgrading to Oracle Identity Manager 11g Release 2 (11.1.2)<br>■ Running the Entitlement List Schedule<br>■ Running the Evaluate User Policies Scheduled Task<br>■ Running Catalog Synchronization<br>■ UMS Notification Provider<br>■ Upgrading User UDF<br>■ Upgrading Application Instances<br>■ Redeploying XIMDD<br>■ Redeploying SPML-DSML<br>■ Customizing Event Handlers<br>■ Upgrading SOA Composites<br>■ Provisioning Oracle Identity Management Login Modules Under WebLogic Server Library Directory<br>■ Authorization Policy Changes |
| 28 | Verify the upgrade. | See, Verifying the Upgrade |

## 6.3 Pre-Upgrade

This section contains the following topics:

- Generating the Pre-Upgrade Report
- Analyzing Pre-Upgrade Report
- Ensuring That getPlatformTransactionManager() Method is Not Used in Custom Code
- Emptying the oimProcessQueue JMS Queue
- Other Prerequisites
- Shutting Down Administration Server and Managed Servers
- Backing Up Oracle Identity Manager 11g Release 1 (11.1.1.5.0)
- Ensuring That JRF is Upgraded

### 6.3.1 Generating the Pre-Upgrade Report

The `Pre-UpgradeReport` utility analyses your existing Oracle Identity Manager 11.1.1.5.0 environment, and provides information about the mandatory prerequisites that you must complete before you upgrade 11.1.1.5.0 environment. The information in the pre-upgrade report is related to the invalid approval policies, requests and event handlers that are affected by the upgrade, list of mandatory Database components that need to be installed before upgrade, cyclic groups in LDAP directory, deprecated authorization policies, and issues in creating potential application instance.

You must run the `PreUpgradeReport` utility before you begin the upgrade process, and address all the issues listed as part of this report with the solution provided in the report. Run this report until no pending issues are listed in the report.

**Note:** It is important to address all the issues listed in the pre-upgrade report, before you can proceed with the upgrade, as upgrade might fail if the issues are not fixed.

Download the pending transaction report utility, as described in the My Oracle Support document ID 1471905.1.

Run `generatePreUpgradeReport.sh` on UNIX, or `generatePreUpgradeReport.bat` on Windows, and provide the following details:

- Oracle Identity Manager schema JDBC URL

  [`jdbc:oracle:thin:@hostname:portnumber/service name`]
- Oracle Identity Manager schema username
- Oracle Identity Manager schema password
- MDS schema JDBC URL

  [`jdbc:oracle:thin:@hostname:portnumber/service name`]
- MDS schema User Name
- MDS schema Password
- Database Administrator username
- SYSDBA password
- Enter report output directory

### 6.3.2 Analyzing Pre-Upgrade Report

The pending transaction report utility generates seven different reports, which includes the information outlined in Table 6–3.

**Note:** You must review all the reports, and perform the tasks described in each of the reports.

*Table 6–3 Pre-Upgrade Utility Reports*

| Report Name | Description | For More Information |
|---|---|---|
| `index.html` | The index.html provides links to all the seven reports generated by the pre-upgrade utility. | - |
| `APPROVALPOLICYPreUpgradeReport.html` | This report lists the request approval policies that has a rule defined on the non existing template. | See, Section 6.3.2.1, "Description of APPROVALPOLICYPreUpgradeReport.html Report". |
| `AUTHORIZATIONPOLICYPreUpgradeReport.html` | This report lists all of the invalid authorization policies. Oracle Identity Manager 11.1.2 does not use the authorization policies created in Oracle Identity Manager 11.1.1.5.0. Therefore, all of the authorization policies created in Oracle Identity Manager 11.1.1.5.0 are invalid in this release. | See, Section 6.3.2.2, "Description of AUTHORIZATIONPOLICYPreUpgradeReport.html Report". |
| `CYCLIC_GROUP_MEMBERSHIP_CHKPreUpgradeReport.html` | This report detects the list of cyclic groups in LDAP.<br>The report includes a list of cyclic groups and instructions to remove cyclic dependency. It is mandatory to remove all cyclic dependencies running in the Oracle Identity Manager 11.1.1.5.0 environment. | See, Section 6.3.2.3, "Description of CYCLIC_GROUP_MEMBERSHIP_CHKPreUpgradeReport.html Report". |
| `EVENT_HANDLERPreUpgradeReport.html` | This report captures all user customizations related to Event Handler in Oracle Identity Manager 11.1.1.5.0. | See, Section 6.3.2.4, "Description of EVENT_HANDLERPreUpgradeReport.html Report". |
| `ORACLE_TEXTPreUpgradeReport.html` | This report lists the mandatory Database components that needs to be installed before you proceed with the upgrade. | See, Section 6.3.2.5, "Description of ORACLE_TEXTPreUpgradeReport.html Report". |
| `PROVISIONINGPreUpgradeReport.html` | This report lists the potential application instance creation issues. | See, Section 6.3.2.6, "Description of PROVISIONINGPreUpgradeReport.html Report". |
| `REQUESTPreUpgradeReport.html` | This report lists any invalid requests and the actions to be taken. | See, Section 6.3.2.7, "Description of REQUESTPreUpgradeReport.html Report". |

### 6.3.2.1 Description of APPROVALPOLICYPreUpgradeReport.html Report

The report `APPROVALPOLICYPreUpgradeReport.html` lists the invalid approval policies. This report contains the following sections:

- Approval Policy rule defined on template
- List of Approval Polices which needs to be updated with custom approval process

- Approval policy based on unsupported request type

This report also contains an additional note on approval policy based on deprecated request type. You must review the report completely, before you start upgrading the Oracle Identity Manager 11.1.1.5.0 environment.

**6.3.2.1.1 Approval Policy rule defined on template** This section lists the Oracle Identity Manager 11.1.1.5.0 approval policies whose rules are defined based on the request template.

The Request templates feature is not supported in Oracle Identity Manager 11.1.2. Therefore, if your Oracle Identity Manager 11.1.1.5.0 contains approval policies having rules based on request template, you must reconfigure the request approval policies by following the steps described in the report.

**6.3.2.1.2 List of Approval Polices which needs to be updated with custom approval process** This section lists the 11.1.1.5.0 approval policies that need to be associated with different approval process before you start the upgrade process.

The approval process `default/ResourceAdministratorApproval`, `default/ResourceAuthorizerApproval` are not supported in 11.1.2. Therefore, if your Oracle Identity Manager 11.1.1.5.0 contains approval policies having these approval process, you must associate them with different approval process.

**6.3.2.1.3 Approval policy based on unsupported request type** This section provides information about the request types that are not supported in 11.1.2.

The following 11.1.1.5.0 request types are not supported in 11.1.2, and they are changed to non-self request type in 11.1.2:

- Self Assign Roles
- Modify Self Profile
- Self Remove Roles
- Self De-Provision Resource
- Self Modify Provisioned Resource
- Self-Request Resource

Self-request type mapping to Non-Self request type is shown Table 6–4.

*Table 6–4 Mapping of Self request type to Non-Self request type*

| Self Request Type | Non-Self Request Type |
|---|---|
| Self-Request Resource | Provision Resource |
| Self Modify Provisioned Resource | Modify Provisioned Resource |
| Self Remove Roles | Remove from Roles |
| Modify Self Profile | Modify User Profile |
| Self De-Provision Resource | De-Provision Resource |
| Self Assign Roles | Assign Roles |

### 6.3.2.2 Description of AUTHORIZATIONPOLICYPreUpgradeReport.html Report

The report `AUTHORIZATIONPOLICYPreUpgradeReport.html` lists the deprecated authorization policies.

Oracle Identity Manager 11.1.2 uses a new authorization policy framework that is standards based, and is used by the entire Oracle stack. Any changes made to authorization policies in Oracle Identity Manager 11.1.1.5 must be reapplied post upgrade.

You must review the table in this report that lists the authorization policies of the 11.1.1.5.0 environment that are deprecated in 11.1.2.

### 6.3.2.3 Description of CYCLIC_GROUP_MEMBERSHIP_CHKPreUpgradeReport.html Report

The report `CYCLIC_GROUP_MEMBERSHIP_CHKPreUpgradeReport.html` provides information about the Cyclic groups in LDAP directory.

Oracle Identity Manager 11.1.2 does not support cyclic groups in the LDAP directory. Therefore, you must remove the cyclic dependency from Oracle Identity Manager 11.1.1.5.0 setup before you proceed with the upgrade. For more information about removing the cyclic groups dependent on LDAP, see Removing Cyclical Groups Dependent on LDAP. The procedure for removing cyclic groups is also described in this report.

#### Removing Cyclical Groups Dependent on LDAP

If the LDAP in your Oracle Identity Manager 11.1.1.5.0 environment has cyclic groups loaded, you must remove the cyclic groups by doing the following:.

1. Use JEXplorer or Softerra LDAP Administrator and navigate to the cyclic groups.
2. Look for **uniquemember** attribute.
3. Remove all values from the attribute.
4. Save the group.
5. Run `LDAPConfigPostSetup.sh` on UNIX and `LDAPConfigPostSetup.bat` on Windows to sync data from LDAP to Oracle Identity Manager database.

#### Example Scenario

If you have cyclic group dependency between two groups: Group1 and Group2, do the following to remove cyclic dependency:

1. Connect to LDAP using JEXplorer or Softerra LDAP.
2. Go to the group container of Group1.
3. Go to the **uniquemember** attribute under Group1.
4. Remove the value of Group2, from unique members, and save the change made.
5. Run `LDAPConfigPostSetup.sh` on UNIX and `LDAPConfigPostSetup.bat` on Windows to synchronize data from LDAP to Oracle Identity Manager database.

### 6.3.2.4 Description of EVENT_HANDLERPreUpgradeReport.html Report

The report `EVENT_HANDLERPreUpgradeReport.html` provides information about event handlers. When you upgrade Oracle Identity Manager 11.1.1.5.0 to Oracle Identity Manager 11.1.2, the customizations made to the OOTB event handlers XMLs in 11.1.1.5.0 will not be preserved in 11.1.2. All the customizations defined in a separate XML (non OOTB) in 11.1.1.5.0 will be preserved in 11.1.2. You must redo all the customizations after upgrading to 11.1.2. This report contains the following sections:

- New Event Handler Added by the customer in the OOTB(11.1.1.5.0) Event Handler Metadata XML

- OOTB(11.1.1.5.0) Event Handler modified by the Customer
- OOTB(11.1.1.5.0) Event Handler deleted by Customer

Refer to the table in the report for more details about the event handlers.

**6.3.2.4.1 New Event Handler Added by the customer in the OOTB(11.1.1.5.0) Event Handler Metadata XML** This section provides information about the new event handlers added in the OOTB (11.1.1.5.0).

The event handler newly added in the OOTB (11.1.1.5.0) Event Handler Metadata XML will not be available after you upgrade to 11.1.2. Oracle Identity Manager 11.1.2 event handlers will replace the 11.1.1.5.0 event handlers. Therefore, you must add the event handler again in a new file after the upgrade.

> **Note:** Do not add new event handler in the same OOTB Event Handler XML. You must create a new XML and add the new event handler to it.

**6.3.2.4.2 OOTB(11.1.1.5.0) Event Handler modified by the Customer** This section provides information about the event handlers that are modified in the OOTB (11.1.1.5.0).

You must redo all the customizations that you did to the event handlers in OOTB (11.1.1.5.0), after you upgrade Oracle Identity Manager 11.1.1.5.0 to 11.1.2.

**6.3.2.4.3 OOTB(11.1.1.5.0) Event Handler deleted by Customer** This section provides information about the event handlers that were deleted in OOTB (11.1.1.5.0).

The deleted event handlers are restored after you upgrade to 11.1.2. Therefore, you must delete them again as per requirement.

### 6.3.2.5 Description of ORACLE_TEXTPreUpgradeReport.html Report

The report `ORACLE_TEXTPreUpgradeReport.html` provides information about the installation status of the mandatory database components.

Before you upgrade Oracle Identity Manager 11.1.1.5.0 to 11.1.2, you must install certain Database components. The table in this report lists the database components that need to be installed before you upgrade. The table also shows the status of the installation, and the solution. Review the table, and perform the actions required.

### 6.3.2.6 Description of PROVISIONINGPreUpgradeReport.html Report

The report PROVISIONINGPreUpgradeReport.html lists the potential application instances creation issues. The report contains the following sections:

- Provisioning, Entitlement, and Access Policy Configuration Details
- List of Resource Objects without Process Form
- List of Resource Objects without ITResource field Type in Process Form
- List of Resource Objects with multiple ITResource Lookup fields in Process Form
- List of Access Policies without ITResource value set in default policy data
- List of Access Policies with Revoke If No Longer Applies flag unchecked
- List of Entitlements stored in Lookup definitions that do not have IT Resource Key in the lookup encode value

**6.3.2.6.1 Provisioning, Entitlement, and Access Policy Configuration Details** This sections describes the steps you must complete before you upgrade Oracle Identity Manager 11.1.1.5.0 to 11.1.2. These steps are related to provisioning, entitlement, and access policy configuration. Complete all the steps described in this section of the report.

**6.3.2.6.2 List of Resource Objects without Process Form** This section provides information about the resource objects in Oracle Identity Manager 11.1.1.5.0 that do not have process form. Each resource object must have a process form associated with it. Therefore, if a resource object is not associated with a process form, you must associate the resource object with a process form before you start the upgrade process. Review the table in this section of the report, that lists the details of the resource objects without process form.

**6.3.2.6.3 List of Resource Objects without ITResource field Type in Process Form** This section provides information about the resource objects without ITResource field type in their respective process forms. Review the table in this section of the report, which contains more details. If your Oracle Identity Manager 11.1.1.5.0 has resource objects without ITResource field in their process forms, do the following:

1. Create appropriate IT resource definition.
2. Create IT resource instance for the same corresponding to the target that is being provisioned.
3. Edit the process form and add a field of type "`ITResource`" to the process form. Set the following properties:

   `Type=`*`IT Resource definition created in step-1`*

   `ITResource=true`
4. Activate the form.
5. Update the IT resource field on existing provisioned accounts using FVC Utility.
6. Once the above steps are completed, you can create application instances corresponding to the Resource Object+ITResource combination.

**6.3.2.6.4 List of Resource Objects with multiple ITResource Lookup fields in Process Form** This section provides information about the resource objects that have multiple lookup fields in their process form. In the Oracle Identity Manager 11.1.1.5.0 environment, if you have resource objects with multiple ITResource set in the process form, you must set the value of the property `ITResource Type` to `true` for at least one of the attributes.

**6.3.2.6.5 List of Access Policies without ITResource value set in default policy data** This section lists the access policies for which the ITResource values of the resource objects should be set in the default policy data. The table in this section lists the access policies in Oracle Identity Manager 11.1.1.5.0 for which ITResource field is missing. You must set the values of ITResurce field for each of the access policy listed in the table.

**6.3.2.6.6 List of Access Policies with Revoke If No Longer Applies flag unchecked** This section lists the access policies that have `Revoke If No Longer Applies` flag unchecked. The table in this section contains the list of access policies that will be updated to `Disable If No Longer Applies`, during upgrade. The table also indicates if tasks for `enable`, `disable`, `revoke` actions are not defined for these policies. You must add the missing tasks before you proceed with the upgrade. Also, if you want the behavior of the policy to change to RNLA checked, you must check the RNLA flag for the respective policy.

**6.3.2.6.7 List of Entitlements stored in Lookup definitions that do not have IT Resource Key in the lookup encode value** This section lists entitlements stored in lookup definitions that do not have IT Resource Key pretended to their encoding values using "~". Entitlements stored in lookup definitions need IT Resource Key prepended to the encoded values using "~". Review the table in this section of the pre-upgrade report, which contains more details.

### 6.3.2.7 Description of REQUESTPreUpgradeReport.html Report

The report `REQUESTPreUpgradeReport.html` lists requests that are affected because of the upgrade. This report contains the following sections:

- Requests with unsupported request stages
- Requests which will be automatically changed to corresponding non-self request type

**6.3.2.7.1 Requests with unsupported request stages** This section lists the requests that are in one of the following unsupported request stages:

- Obtaining Template Approval
- Template Approval Approved
- Template Approval Rejected
- Template Approval Auto Approved

Manual intervention is required to move these requests to the next stage by approving, withdrawing, or closing such requests. Otherwise, requests are moved to `request closed` stage as part of the upgrade.

Review the list of requests that are in the unsupported request stage.

**6.3.2.7.2 Requests which will be automatically changed to corresponding non-self request type**

This section lists the requests that are based on one of the following request types will be changed to the corresponding non-self request type after the upgrade:

- Self Assign Roles
- Modify Self Profile
- Self Remove Roles
- Self De-Provision Resource
- Self Modify Provisioned Resource
- Self-Request Resource

Request types for these requests are automatically changed to the corresponding non-self request type as part of the upgrade.

Self-request type mapping to non-self request type is shown in Table 6–5:

*Table 6–5 Mapping of Self-Request Type to Non-Self Request Type*

| Self request type | Non-Self request type |
|---|---|
| Self-Request Resource | Provision Resource |
| Self Modify Provisioned Resource | Modify Provisioned Resource |
| Self Remove Roles | Remove from Roles |

*Table 6–5 (Cont.) Mapping of Self-Request Type to Non-Self Request Type*

| Self request type | Non-Self request type |
|---|---|
| Modify Self Profile | Modify User Profile |
| Self De-Provision Resource | De-Provision Resource |
| Self Assign Roles | Assign Roles |

### 6.3.3 Ensuring That getPlatformTransactionManager() Method is Not Used in Custom Code

Ensure that the method `getPlatformTransactionManager()` is not used in the custom event handler code, as this method is not available in 11.1.2.

If you are using the method getPlatformTransactionManager() in the custom event handler code, set the attribute `tx` to `TRUE` in the event handler XML definition.

For more information on setting the attributes in the event handler XML definition, see "Defining Custom Events Definition XML" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

### 6.3.4 Emptying the oimProcessQueue JMS Queue

Offline Provisioning is not supported in Oracle Identity Manager 11.1.2, as it is no longer needed on Oracle Identity Manager 11.1.2.

Empty the `oimProcessQueue` JMS queue to ensure that JMS messages are processed before you start upgrading. To do so, complete the following:

1. Shut down applications to disable accessing of Oracle Identity Manager offline provisioning by end-users, SPML, and API clients.
2. Monitor the `oimProcessQueue` JMS queue from the Weblogic Administration Console and allow Oracle Identity Manager to run, till o`imProcessQueue` JMS queue is empty.

### 6.3.5 Other Prerequisites

This is a list of checks you must run and set before you begin upgrading:

- Check if `oracle.soa.worklist.webapp` is targeted to Oracle Identity Manager server in 11.1.1.5.0. If not, targeted it to Oracle Identity Manager Managed Server.
- The OOTB applications in Oracle Identity Manager are deployed in `NO_STAGE` mode. Check if `oracle.idm.uishell` is in `No Stage` mode. If `oracle.idm.uishell` is in `Stage` mode, you must re-deploy it.

  Complete the following steps to change the mode to `No Stage`:

  1. Set the *`WL_HOME`* and *`OIM_HOME`*.
  2. Undeploy `oracle.idm.uishell` by running the following command:

     ```
     java -cp $WL_HOME/server/lib/weblogic.jar weblogic.Deployer
     -adminurl t3://localhost:8005 -username weblogic -password
     weblogic1 -undeploy -name oracle.idm.uishell
     ```

  3. Deploy `oracle.idm.uishell` in stage mode by running the following command:

     ```
     java -cp $WL_HOME/server/lib/weblogic.jar weblogic.Deployer
     -adminurl t3://localhost:8005 -username weblogic -password
     ```

```
weblogic1 -deploy -name oracle.idm.uishell -source $OIM_
HOME/modules/oracle.idm.uishell_11.1.1/oracle.idm.uishell.war
-nostage -library -targets AdminServer,$OIM_SERVER_NAME
```

- Ensure that all pending requests are addressed before you upgrade.
- In case of a migrated, upgraded, or restored database in the Oracle Identity Manager enviornment, you must synchronize all the Oracle Identity Manager Schema Privileges (SYSTEM and OBJECT Grants) from the source to the target (restored) schema by doing the following:

  1. Capture the OIM Database Schema user constituent grants from the source schema by executing the following SQLs as `SYS` database user:

     – `SELECT DBMS_METADATA.GET_GRANTED_DDL ('SYSTEM_GRANT','<OIM_Schema_Name>') FROM DUAL;`

     – `SELECT DBMS_METADATA.GET_GRANTED_DDL ('OBJECT_GRANT', '<OIM_Schema_Name>') FROM DUAL;`

  2. In the schema restoration phase prior to schema upgrade, execute the grants output of the SQLs captured in step-1, as post schema restoration step.

  3. Recompile any `INVALID` objects in the OIM schema using the following steps:

     a. Identify `INVALID` schema objects as `SYS` user by running the following SQL:

     ```
     SELECT owner,object_type,object_name,status FROM dba_objects WHERE
     status = 'INVALID' AND owner in ('<OIM_Schema_Name1>') ORDER BY
     owner, object_type, object_name;
     ```

     b. Compile the `INVALID` schema objects using any appropriate method. The following is an example of compiling `INVALID` schema objects by executing the method `UTL_RECOMP` as `SYS` user for the OIM schema:

     ```
     UTL_RECOMP.recomp_serial('<OIM_Schema_Name>');
     ```

     ```
     END;
     ```

     Repeat step-a until there are no `INVALID` objects.

     > **Note:** For information on schema backup and restoration using Data Pump Client Utility for Oracle Identity Manager 11*g* Release 1, see My Oracle Support document ID 1359656.1.
     >
     > For information on schema backup and restoration using Data Pump Client Utility for Oracle Identity Manager 11*g* Release 2, see My Oracle Support document ID 1492129.1.

### 6.3.6 Ensuring That JRF is Upgraded

Before starting the upgrade process, you must ensure that Java Required Files (JRF) is upgraded. To do this, complete the following steps:

1. Log in to the WebLogic Administration console using the following URL:

   `http://host:port/console`

   In this URL, *`host`* refers to the name of the host on which WebLogic Administration Server is running, and *`port`* refers to the port number.

2. Click **Deployments** on the left navigation pane for the *`OIM_Domain`*.

3. Ensure that the following libraries are present:

- `oracle.adf.desktopintegration(1.0,11.1.1.2.0)`
- `oracle.adf.desktopintegration.model(1.0,11.1.1.2.0)`
- `oracle.bi.adf.model.slib(1.0,11.1.1.2.0)`
- `oracle.bi.adf.view.slib(1.0,11.1.1.2.0)`
- `oracle.bi.adf.webcenter.slib(1.0,11.1.1.2.0)`
- `oracle.bi.composer(11.1.1,0.1)`
- `oracle.bi.jbips(11.1.1,0.1)`

If the above libraries are not present, you must upgrade JRF. For more information about upgrading JRF, see "Updating Fusion Middleware Shared Libraries" in the *Oracle Fusion Middleware Patching Guide*.

## 6.3.7 Shutting Down Administration Server and Managed Servers

The upgrade process involves changes to the binaries and to the schema. Therefore, before you begin the upgrade process, you must shut down the Managed Servers and the Administration Server.

To shut down the Servers, do the following:

### Stopping Managed Servers

To stop the Managed Servers, do the following:

**On UNIX**:

1. Move from your present working directory to the `<MW_HOME>/user_projects/domains/<domain_name>/bin` directory by running the following command on the command line:

   ```
   cd <MW_HOME>/user_projects/domains/<domain_name>/bin
   ```

2. Run the following command to stop the servers:

   ```
   ./stopManagedWebLogic.sh <server_name> <admin_url> <user_name>
   <password>
   ```

   where

   `<server_name>` is the name of the Managed Server.

   `<admin_url>` is URL of the administration console. Specify it in the format `http://<host>:<port>/console`. Specify only if the WebLogic Administration Server is on a different computer.

   `<user_name>` is the username of the WebLogic Administration Server.

   `<password>` is the password of the WebLogic Administration Server.

**On Windows**:

1. Move from your present working directory to the `<MW_HOME>\user_projects\domains\<domain_name>\bin` directory by running the following command on the command line:

   ```
   cd <MW_HOME>\user_projects\domains\<domain_name>\bin
   ```

2. Run the following command to stop the Managed Servers:

   ```
   stopManagedWebLogic.cmd <server_name> <admin_url> <username> <password>
   ```

   where

`<server_name>` is the name of the Managed Server.

`<admin_url>` is URL of the administration console. Specify it in the format `http://<host>:<port>/console`. Specify only if the WebLogic Administration Server is on a different computer.

`<username>` is the username of the WebLogic Administration Server.

`<password>` is the password of the WebLogic Administration Server.

For more information, see "Stopping the Stack" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

#### Stopping the Administration Server

To stop the Administration Server, do the following:

**On UNIX**:

Run the following command:

```
cd <MW_HOME>/user_projects/domains/<domain_name>/bin
```

```
./stopWebLogic.sh
```

**On Windows**:

Run the following command:

```
cd <MW_HOME>\user_projects\domains\<domain_name>\bin
```

```
stopWebLogic.cmd
```

### 6.3.8 Backing Up Oracle Identity Manager 11*g* Release 1 (11.1.1.5.0)

You must back up your old Oracle Identity Manager 11.1.1.5.0 environment before you upgrade to Oracle Identity Manager 11*g* Release 2 (11.1.2).

After stopping the servers, back up the following:

- *MW_HOME* directory, including the Oracle Home directories inside Middleware Home
- Domain Home directory
- Oracle Identity Manager schemas
- MDS schema
- ORASDPM schema
- SOAINFRA schemas

For more information about backing up schemas, see *Oracle Database Backup and Recovery User's Guide*.

## 6.4 Upgrade Procedure

This section describes different tasks involved in the upgrade process, like upgrading Oracle Identity Manager and Oracle SOA Suite 11.1.1.5.0 binaries, creating 11.1.2 schemas, configuring the security store, upgrading the Oracle Identity Manager middle tier, verifying the upgrade and so on. The tasks in this section should be performed after you complete all the prerequisites described in section Pre-Upgrade.

This section contains the following topics:

- Optional: Upgrading Oracle WebLogic Server

- Upgrading Oracle SOA Suite Used by Oracle Identity Manager
- Upgrading Oracle Identity Manager 11g Release 2 (11.1.2)
- Creating Oracle Platform Security Services Schema
- Extending Oracle Identity Manager 11.1.1.5.0 Component Domains with OPSS Template
- Upgrading Oracle Platform Security Services
- Configuring OPSS Security Store
- Upgrading Oracle Identity Management Schemas Using Patch Set Assistant
- Starting the Administration Server and SOA Managed Servers
- Setting Environment Variables
- Upgrading Oracle Identity Manager Middle Tier
- Verifying Oracle Identity Manager Middle Tier Upgrade
- Changing the Deployment Order of Oracle Identity Manager EAR
- Restarting the Administration Server and SOA Managed Server
- Patching Oracle Identity Management MDS Metadata
- Upgrading Oracle Identity Manager Design Console
- Upgrading Oracle Identity Manager Remote Manager
- Configuring BI Publisher Reports

### 6.4.1 Optional: Upgrading Oracle WebLogic Server

> **Note:** Upgrading Oracle WebLogic Server is not mandatory. However, Oracle recommends that you upgrade Oracle WebLogic Server to 10.3.6.

You can upgrade WebLogic Server 10.3.5 to Oracle WebLogic Server 10.3.6 by using the WebLogic 10.3.6 Upgrade Installer. Complete the following steps:

1. Download the WebLogic 10.3.6 Upgrade Installer from Oracle Technology Network.

   For more information, see "Downloading an Upgrade Installer From My Oracle Support" in the *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*.

2. Run the Upgrade Installer in graphical mode to upgrade your WebLogic Server.

   For more information, see "Running the Upgrade Installer in Graphical Mode" in the *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*.

### 6.4.2 Upgrading Oracle SOA Suite Used by Oracle Identity Manager

You must update your existing Oracle SOA 11.1.1.5.0 to Oracle SOA 11.1.1.6.0. To do so, complete the tasks listed in Table 6–6:

***Table 6–6 Tasks to Update SOA***

| Task | For More Information |
|---|---|
| Obtain the Oracle SOA Suite 11.1.1.6.0 installer. | See, *Oracle Fusion Middleware Download, Installation, and Configuration ReadMe* |
| Start the installer. | See, "Start the Installer" in the *Oracle Fusion Middleware Patching Guide* |
| Upgrade SOA to the latest version. | See, "Patch Set Installer Instructions" in the *Oracle Fusion Middleware Patching Guide* |
| Upgrade your SOA schemas using Patch Set Assistant. | See, Upgrading Schemas using Patch Set Assistant |
| Perform post-patching tasks only after starting the Administration Server and the SOA Managed Servers as described in Section 6.4.9, "Starting the Administration Server and SOA Managed Servers".<br>Do not perform the post-patching tasks for SOA until you complete all the tasks till Section 6.4.9. | See, "Post-Patching Tasks" for Oracle SOA Suite |

### 6.4.2.1 Upgrading Schemas using Patch Set Assistant

This section consists of the following topics:

- Checking Your Database and Schemas
- Starting Patch Set Assistant
- Using the Patch Set Assistant Graphical Interface
- Verifying Schema Upgrade

**6.4.2.1.1 Checking Your Database and Schemas** Before running Patch Set Assistant, you should make sure that your database is running and that the schemas are supported. To check this, run the following SQL command:

```
SELECT OWNER, VERSION, STATUS, UPGRADED FROM SCHEMA_VERSION_REGISTRY;
```

If the number in the "VERSION" column is 11.1.1.5.0, then the schema is supported for upgrade.

**6.4.2.1.2 Starting Patch Set Assistant** To start Patch Set Assistant, do the following:

#### On UNIX:

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

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

2. Run the following command:

   ```
   ./psa
   ```

**On Windows:**

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

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

2. Execute the following command:

   ```
   psa.bat
   ```

##### 6.4.2.1.3 Using the Patch Set Assistant Graphical Interface

> **Note:** Even if you upgrade your schemas from 11.1.1.5.0 to 11.1.2, you will see the Patch Set Assistant version number as 11.1.1.6.1 on the **Welcome** screen.
>
> This is not an error. The discrepancy is caused by a difference between how Patch Set Assistant and Identity Access Management releases are tracked internally.

After starting the Patch Set Assistant Installer, follow the instructions on the screen to update your schemas.

Follow the instructions in Table 6–7 to update your schemas:

***Table 6–7 Patch Set Assistant Screens***

| Screen | Description |
|---|---|
| Welcome | This page introduces you to the Patch Set Assistant. |
| Select Component | Select the top-level component you want to upgrade. |
| Prerequisite | Verify that you have satisfied the database prerequisites. |
| Schema | Specify your database credentials to connect to your database, then select the schema you want to update.<br>Note that this screen appears once for each schema that must be updated as a result of the component you selected on the Select Component screen. |
| Examine | This page displays the status of the Patch Set Assistant as it examines each component schema. Verify that your schemas have a "successful" indicator in the Status column. |
| Upgrade Summary | Verify that the schemas are the ones you want to upgrade. |
| Upgrade Progress | This screen shows the progress of the schema upgrade. |
| Upgrade Success | Once the upgrade is successful, you get this screen. |

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

**On UNIX:**

```
<MW_HOME>/oracle_common/upgrade/logs/psa/psatimestamp.log
```

**On Windows:**

```
<MW_HOME>\oracle_common\upgrade\logs\psa\psatimestamp.log
```

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

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

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

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

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

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

## 6.4.3 Upgrading Oracle Identity Manager 11*g* Release 2 (11.1.2)

To upgrade Oracle Identity Manager, you must use the Oracle Identity and Access Management 11*g* Release 2 (11.1.2) Installer. During the procedure, point the Middleware Home to your existing 11.1.1.5.0 Middleware Home. Your Oracle Home is upgraded from 11.1.1.5.0 to 11.1.2.

This section contains the following topics:

- Obtaining the Software
- Starting the Oracle Identity and Access Management 11g Release 2 (11.1.2) Installer
- Installing Oracle Identity and Access Management 11g Release 2 (11.1.2)

### 6.4.3.1 Obtaining the Software

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

### 6.4.3.2 Starting the Oracle Identity and Access Management 11*g* Release 2 (11.1.2) Installer

This topic explains how to start the Oracle Identity and Access Management 11.1.2 Installer.

**Notes:**

- If you are installing 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 from the location where you extracted the contents of the installer (for example, `<unzipped_folder>/Disk1`) by doing the following:

**On UNIX**:

Run the following command:

```
./runInstaller -jreLoc <complete path to the JRE directory>
```

For example:

```
./runInstaller -jreLoc <MW_HOME>/jdk160_29/jre
```

**On Windows**:

Run the following command:

```
setup.exe -jreLoc <complete path to the JRE directory>
```

For example:

```
setup.exe jreLoc <MW_HOME>\jdk160_29\jre
```

---

**Note:** 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 is not created under your Middleware Home. You must enter the absolute path to the JRE folder from where your JDK is located.

---

#### 6.4.3.3 Installing Oracle Identity and Access Management 11*g* Release 2 (11.1.2)

Use the Oracle Identity and Access Management 11.1.2 Installer to upgrade Oracle Identity Management 11.1.1.5.0 to Oracle Identity Management 11.1.2:

1. After you start the Installer, the Welcome screen appears.
2. Click **Next** on the **Welcome** screen. The **Install Software Updates** screen appears. Select whether or not you want to search for updates. Click **Next**.
3. The **Prerequisite Checks** screen appears. If all prerequisite checks pass inspection, click **Next**. The **Specify Installation Location** screen appears.
4. On the **Specify Installation Location** screen, point the Middleware Home to your existing 11.1.1.5.0 Middleware Home installed on your system.
5. In the **Oracle Home Directory** field, specify the path of the existing Oracle Identity and Access Management Home. This directory is also referred to as `<IAM_HOME>` in this book.

   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 you want to proceed with 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 **Help** on the installation wizard screens.

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

This installation process copies the 11.1.2 Oracle Identity and Access Management software to your system.

For more information, see "Installing and Configuring Oracle Identity and Access Management (11.1.2)" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

### 6.4.4 Creating Oracle Platform Security Services Schema

You must create Oracle Platform Security Services (OPSS) schema using Repository Creation Utility (RCU), as Oracle Identity Manager upgrade process involves OPSS schema policy store changes. Keys, roles, permissions, and other artifacts used by the applications must migrate to the policy store.

To create OPSS schema using Repository Creation utility, do the following:

1. Obtain the RCU.

   For information about obtaining the RCU software, see "Obtaining RCU" in the *Oracle Fusion Middleware Repository Creation Utility User's Guide*.

2. Start the RCU.

   For information about starting the RCU, see "Starting RCU" in the *Oracle Fusion Middleware Repository Creation Utility User's Guide*.

3. Create the OPSS schema.

   For information about creating schemas, see "Creating Schemas" in the *Oracle Fusion Middleware Repository Creation Utility User's Guide*.

   **Note:** In the **Select Components** screen, expand **AS Common Schemas** and select **Oracle Platform Security Services**. Make sure you do not select any other components.

### 6.4.5 Extending Oracle Identity Manager 11.1.1.5.0 Component Domains with OPSS Template

Oracle Identity Manager 11.1.2 uses the database to store Oracle Entitlements Server policies. This requires extending the 11.1.1.5.0 Oracle Identity Manager domain to include the OPSS data source.

To do so, complete the following steps:

1. Run the following command to launch the Oracle Fusion Middleware configuration wizard:

   **On UNIX:**

   ```
   ./config.sh
   ```

   It is located in the `<MW_HOME>/<Oracle_IDM1>/common/bin` directory.

   **On Windows:**

   ```
   config.cmd
   ```

   It is located in the `<MW_HOME>\<Oracle_IDM1>\common\bin` directory.

2. On the **Welcome** screen, select the **Extend an existing WebLogic domain** option. Click **Next**.

3. On the **Select a WebLogic Domain Directory** screen, browse to the directory that contains the WebLogic domain in which you configured the components. Click **Next**. The **Select Extension Source** screen is displayed.
4. On the **Select Extension Source** screen, select the **Oracle Platform Security Service - 11.1.1.0 [Oracle_IDM1]** option. After selecting the domain configuration options, click **Next**.
5. The **Configure JDBC Data Sources** screen is displayed. Configure the opssDS data source, as required. After the test succeeds, the **Configure JDBC Component Schema** screen is displayed.
6. On the **Configure JDBC Component Schema** screen, select the **Oracle Platform Security Services** schema.

   You can set values for Schema Owner, Schema Password, Database and Service, Host Name, and Port. Click **Next**.

   The **Test JDBC Component Schema** screen is displayed. After the test succeeds, the **Select Optional Configuration** screen is displayed.
7. On the **Select Optional Configuration** screen, you can configure Managed Servers, Clusters, and Machines and Deployments and Services. Do not select anything as you have already configured in your Oracle Identity Manager 11.1.1.5.0 environment. Click **Next**.
8. On the **Configuration Summary** screen, review the domain configuration, and click **Extend** to start extending the domain.

Your existing Oracle Identity Manager domain is extended to support Oracle Platform Security Services (OPSS).

### 6.4.6 Upgrading Oracle Platform Security Services

To upgrade Oracle Platform Security Services (OPSS) schema, do the following:

**On UNIX:**

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

   ```
   cd <MW_HOME>/oracle_common/common/bin
   ```
2. Run the following command to launch the WebLogic Scripting Tool (WLST):

   ```
   ./wlst.sh
   ```
3. At the WLST prompt, run the following command:

   ```
   upgradeOpss(jpsConfig="existing_jps_config_file", jaznData="system_
   jazn_data_file")
   ```

   For example:

   ```
   upgradeOpss(jpsConfig="<MW_HOME>/user_
   projects/domains/<DOMAIN>/config/fmwconfig/jps-config.xml",jaznData="<M
   W_HOME>/oracle_common/modules/oracle.jps_11.1.1/domain_
   config/system-jazn-data.xml")
   ```
4. Exit the WLST console using the `exit()`command.

**On Windows:**

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

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

2. Run the following command to launch the WebLogic Scripting Tool (WLST):

   ```
   wlst.cmd
   ```

3. At the WLST prompt, run the following command:

   ```
   upgradeOpss(jpsConfig="existing_jps_config_file", jaznData="system_
   jazn_data_file")
   ```

   For example:

   ```
   upgradeOpss(jpsConfig="<MW_HOME>\\user_projects\\domains\\base_
   domain\\config\\fmwconfig\\jps-config.xml",jaznData="<MW_HOME>\\oracle_
   common\\modules\\oracle.jps_11.1.1\\domain_
   config\\system-jazn-data.xml")
   ```

4. Exit the WLST console using the `exit()` command.

Table 6–8 describes the parameters you need to specify on the command line:

***Table 6–8 Parameters for Upgrading OPSS***

| Parameter | Description |
|---|---|
| `jpsConfig` | Specify the path to the `jps-config.xml` file in your 11.1.2 installation. The following example shows the complete path:<br>On UNIX, it is located in the `<MW_HOME>/user_projects/domains/base_domain/config/fmwconfig/jps-config.xml` directory.<br>On Windows, it is located in the `<MW_HOME>\user_projects\domains\base_domain\config\fmwconfig\jps-config.xml` directory. |
| `jaznData` | Specify the path to the system-jazn-data.xml file in your 11.1.2 installation. The following example shows the complete path:<br>On UNIX, it is located in the `<MW_HOME>/oracle_common/modules/oracle.jps_11.1.1/domain_config/system-jazn-data.xml` directory.<br>On Windows, it is located in the `<MW_HOME>\oracle_common\modules\oracle.jps_11.1.1\domain_config\system-jazn-data.xml` directory. |

## 6.4.7 Configuring OPSS Security Store

You must configure the database Security Store as it is the only security store type supported by Oracle Identity and Access Management 11g Release 2 (11.1.2). This is done by running the `configureSecurityStore.py` script.

For information about configuring Oracle Platform Security Services, see "Configuring Database Security Store for an Oracle Identity and Access Management Domain" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

## 6.4.8 Upgrading Oracle Identity Management Schemas Using Patch Set Assistant

You must upgrade Oracle Identity Manager schema using Patch Set Assistant (PSA). When you select the Oracle Identity Manager Schema, it automatically selects all dependent schemas and upgrades them too.

Complete the tasks listed in Table 6–9 to upgrade your schemas:

*Table 6–9 Upgrade Oracle Identity Manager Schemas Using PSA*

| Task | For More Information |
|---|---|
| Check the database and schemas in your system. | See, Checking Your Database and Schemas |
| Start the Patch Set Assistant to run the Installer. | See, Starting Patch Set Assistant |
| Use the Patch Set Assistant's graphic interface to upgrade your schemas to the current version. | See, Using the Patch Set Assistant Graphical Interface |
| Verify the schemas you have upgraded. | See, Verifying Schema Upgrade and Version Numbers After Upgrading Schemas |

### 6.4.8.1 Version Numbers After Upgrading Schemas

Run `select version,status,upgraded from schema_version_registry where owner=<SCHEMA_NAME>;` and ensure that the version numbers are upgraded, as listed in Table 6–10:

*Table 6–10 Component Version Numbers After Upgrading the Schemas*

| Component | Version No. |
|---|---|
| APM | 11.1.1.3.0 |
| MDS | 11.1.1.6.0 |
| Oracle Identity Manager | 11.1.2.0.0 |
| ORASDPM | 11.1.1.2.0 |
| SOAINFRA | 11.1.1.6.0 (Make sure that you have upgraded SOA schemas as described in Section 6.4.2.1, "Upgrading Schemas using Patch Set Assistant") |

## 6.4.9 Starting the Administration Server and SOA Managed Servers

**Note:** Do not start the Oracle Identity Manager Managed Servers.

After the upgrade is complete, start the WebLogic Administration Server, the Administration Server for the domain that contains Oracle Identity Management, and SOA Managed Servers.

### Starting the Administration

To start the Administration Server, do the following:

**On UNIX**:

Run the following command:

```
cd <MW_HOME>/user_projects/domains/<domain_name>/bin
```

```
./startWebLogic.sh
```

**On Windows**:

Run the following command:

```
cd <MW_HOME>\user_projects\domains\<domain_name>\bin
```

```
startWebLogic.cmd
```

### Starting Managed Servers

To start the Managed Servers, do the following:

**On UNIX**:

1. Move from your present working directory to the `<MW_HOME>/user_projects/domains/<domain_name>/bin` directory by running the following command on the command line:

   ```
   cd <MW_HOME>/user_projects/domains/<domain_name>/bin
   ```

2. Run the following command to start the SOA Managed Servers:

   ```
   ./startManagedWebLogic.sh <managed_server_name> <admin_url> <user_name>
   <password>
   ```

   where

   `<managed_server_name>` is the name of the Managed Server

   `<admin_url>` is URL of the administration console. Specify it in the format `http://<host>:<port>/console`. Specify only if the WebLogic Administration Server is on a different computer.

   `<user_name>` is the username of the WebLogic Administration Server.

   `<password>` is the password of the WebLogic Administration Server.

**On Windows**:

1. Move from your present working directory to the `<MW_HOME>\user_projects\domains\<domain_name>\bin` directory by running the following command on the command line:

   ```
   cd <MW_HOME>\user_projects\domains\<domain_name>\bin
   ```

2. Run the following command to start the SOA Managed Servers:

   ```
   startManagedWebLogic.cmd <managed_server_name> <admin_url> <user_name>
   <password>
   ```

   where

   `<managed_server_name>`  is the name of the Managed Server.

   `<admin_url>` is URL of the administration console. Specify it in the format `http://<host>:<port>/console`. Specify only if the WebLogic Administration Server is on a different computer.

   `<user_name>` is the username of the WebLogic Administration Server.

   `<password>` is the password of the WebLogic Administration Server.

For more information, see "Starting the Stack" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

## 6.4.10 Setting Environment Variables

You must set environment variables, before you upgrade the Oracle Identity Manager middle tier. Follow the steps described in Table 6–11 to set the environment variables.

***Table 6–11 Environment Variables for Oracle Identity Manager***

| Environment Variable | Values |
|---|---|
| `MW_HOME` | Specify the path to the Oracle Identity Manager's Middleware Home. The following example shows the complete path:<br>On UNIX, it is located in the `/oracle/Middleware` directory.<br>On Windows, it is located in the `\oracle\Middleware` directory. |
| `WL_HOME` | Specify the path to the Oracle WebLogic Server home. The following example shows the complete path:<br>On UNIX, it is located in the `oracle/Middleware/wlserver_10.3` directory.<br>On Windows, it is located in the `oracle\Middleware\wlserver_10.3` directory. |
| `JAVA_HOME` | Specify the path to the Java home. The following example shows the complete path:<br>On UNIX, it is located in the `<MW_HOME>/jdk160_29/` directory.<br>On Windows, it is located in the `<MW_HOME>\jdk160_29\` directory. |
| `OIM_HOME` | Specify the path to the Oracle Identity Manager 11*g* Release 1 (11.1.1.5.0) Server home. The following example shows the complete path:<br>On UNIX, it is located in the `<MW_HOME>/<Oracle_IDM1>/` directory.<br>On Windows, it is located in the `<MW_HOME>\<Oracle_IDM1>\` directory. |
| `SOA_HOME` | Specify the path to the SOA Home. The following example shows the complete path:<br>On UNIX, it is located in the `<MW_HOME>/<Oracle_SOA1>/` directory.<br>On Windows, it is located in the `<MW_HOME>\<Oracle_SOA1>\` directory. |

## 6.4.11 Upgrading Oracle Identity Manager Middle Tier

This section contains the following topics:

- Additional Task for Windows 64-Bit Users Before Upgrading Middle Tier
- Upgrading Oracle Identity Manager Middle Tier Using Property File
- Upgrading Oracle Identity Manager Middle Tier on the Command Line

### 6.4.11.1 Additional Task for Windows 64-Bit Users Before Upgrading Middle Tier

If you are running the upgrade in a 64-bit Windows platform, complete the following task to run Middle Tier upgrade successfully:

1. Add a *JAVA_HOME* entry to the environment variable pointing to a JDK installation, not to a JRE installation.

**Note:** This path should be without spaces or like `C:\Progra~1\Java\jdk1.6.0_29`.

2. Hard code the value of *JAVA_HOME* in `<WL_HOME>\server\bin\setWLSEnv.cmd` file to avoid any Middle Tier upgrade failures.

#### 6.4.11.2 Upgrading Oracle Identity Manager Middle Tier Using Property File

**Note:** The execution is reentrant and will resume with correct execution even if there is any interruption in between.

To upgrade Oracle Identity Manager Middle Tier using property file, complete the following steps:

**On UNIX:**

1. Move from your present working directory to the `<OIM_HOME>/server/bin` directory by running the following command on the command line:

   ```
   cd <OIM_ORACLE_HOME>/server/bin
   ```

2. Change the path to `<OIM_ORACLE_HOME>/bin`.
3. Open the following file in a text editor:

   ```
   oim_upgrade_input.properties
   ```

4. Add the parameters, as listed in Table 6–12.
5. Move from your present working directory to the `<MW_HOME>/Oracle_IDM1/server/bin` directory by running the following command on the command line:

   ```
   cd <MW_HOME>/Oracle_IDM1/server/bin
   ```

6. Run the following command:

   ```
   ./OIMUpgrade.sh
   ```

**Note:** The following warning is displayed:

```
[WARN ][jrockit] PermSize=128M ignored: Not a valid option
for JRockit
```

```
[WARN ][jrockit] MaxPermSize=256M ignored: Not a valid
option for JRockit
```

You can ignore this message.

**On Windows:**

1. Move from your present working directory to the `<OIM_HOME>\server\bin` directory by running the following command on the command line:

   ```
   cd <OIM_ORACLE_HOME>\server\bin
   ```

2. Change the path to `<OIM_ORACLE_HOME>\bin`.
3. Open the following file in a text editor:

```
oim_upgrade_input.properties
```

4. Add the parameters, as listed in Table 6–12.

5. Move from your present working directory to the `<MW_HOME>\<OIM_ORACLE_HOME>\server\bin` directory by running the following command on the command line:

   ```
   cd <MW_HOME>\<OIM_ORACLE_HOME>\server\bin
   ```

6. Run the following command:

   ```
   OIMUpgrade.bat
   ```

> **Note:** The following warning is displayed:
>
> ```
> [WARN ][jrockit] PermSize=128M ignored: Not a valid option
> for JRockit
> ```
>
> ```
> [WARN ][jrockit] MaxPermSize=256M ignored: Not a valid
> option for JRockit
> ```
>
> You can ignore this message.

***Table 6–12 Oracle Identity Manager Middle Tier Upgrade Parameters***

| Parameter | Description |
|---|---|
| `oim.jdbcurl` | Specify the Oracle Identity Manager JDBC URL. |
| `oim.oimschemaowner` | Specify the Oracle Identity Manager schema owner. |
| `oim.oimmdsjdbcurl` | Specify the MDS JDBC URL. |
| `oim.mdsschemaowner` | Specify the MDS schema owner name. |
| `oim.adminhostname` | Specify the Oracle WebLogic Server Administration host name. |
| `oim.adminport` | Specify the Oracle WebLogic Server Administration port. |
| `oim.adminUserName` | Specify the username that is used to log in to the Oracle WebLogic Server Administration Console. |
| `oim.soahostmachine` | Specify the SOA host name where SOA Server is running. |
| `oim.soaportnumber` | Specify the SOA Server port. |
| `oim.soausername` | Specify the SOA Managed Server username. |
| `oim.domain` | Specify the Oracle Identity Manager domain location. |

### Example Parameters

```
oim.jdbcurl=db.example.com:5521/dbmode.example.com
oim.oimschemaowner=test_oim23
oim.oimmdsjdbcurl=db.example.com:5521/dbmode.example.com
oim.mdsschemaowner=test_mds
oim.adminport=7001
oim.adminhostname=<oim_host>:<oim_port>
oim.adminUserName=weblogic
oim.soahostmachine=<oim_soa_host>:<oim_soa_port>
oim.soaportnumber=8001
oim.soausername=weblogic
oim.domain=/<MW_HOME>/user_projects/domains/<base_domain>
```

#### 6.4.11.3 Upgrading Oracle Identity Manager Middle Tier on the Command Line

You can also upgrade Oracle Identity Manager Middle Tier by running the `OIMUpgrade` command on the Command Line Interface (CLI):

**On UNIX:**

1. Move from your present working directory to the `<MW_HOME>/<OIM_ORACLE_HOME>/server/bin` directory by running the following command on the command line:

   ```
   cd <MW_HOME>/<OIM_ORACLE_HOME>/server/bin
   ```

2. Run the following command:

   ```
   ./OIMUpgrade.sh <oim connection string> <oim_schema_owner_name> <mds
   conection string> <mds schema owner name> <admin_hostname> <admin_port>
   <admin_username> <soa_host_machine_name> <soa_port_number> <soa_
   username> <domain_location_directory>
   ```

   Specify the parameters, as listed in Table 6–12.

**On Windows:**

1. Move from your present working directory to the `<MW_HOME>\<OIM_ORACLE_HOME>\server\bin` directory by running the following command on the command line:

   ```
   cd <MW_HOME>\<OIM_ORACLE_HOME>\server\bin
   ```

2. Run the following command:

   ```
   OIMUpgrade.bat <oim connection string> <oim_schema_owner_name> <mds_
   conection_string> <mds_schema_owner_name> <admin_hostname> <admin_port>
   <admin_username> <soa_host_machine_name> <soa_port_number> <soa_
   username> <domain_location_directory>
   ```

   Specify the parameters, as listed in Table 6–12.

### 6.4.12 Verifying Oracle Identity Manager Middle Tier Upgrade

Complete the following steps to verify the Oracle Identity Manager Middle Tier upgrade:

1. Verify the log files at the following location, by looking for error or warning messages:

   **On UNIX:**

   ```
   <OIM_HOME>/server/upgrade/logs/MT
   ```

   **On Windows:**

   ```
   <OIM_HOME>\server\upgrade\logs\MT
   ```

   The following log files are generated:

   - `ant_JRF.log`
   - `ant_PatchClasspath.log`
   - `OIMUpgrade<timestamp>.log`
   - `SeedSchedulerData.log`

   No error message is displayed if the middle tier upgrade was successful.

2. `OIMupgrade.sh` creates a detailed report. Complete the following steps to verify the Oracle Identity Manager Middle Tier upgrade:

   a. Go to the following path:

      **On UNIX:**

      `<Oracle_IDM1>/server/upgrade/logs/MT/oimUpgradeReportDir`

      **On Windows:**

      `<Oracle_IDM1>\server\upgrade\logs\MT\oimUpgradeReportDir`

   b. Click **index.html**.

      This contains list of all Oracle Identity Manager features and upgrade status of the last middle tier run, in a table format.

   c. Click on the corresponding link of each feature for a detailed feature report.

***Table 6–13 Middle Tier Upgrade Report***

| Feature | Name | Description |
|---|---|---|
| | `index.html` | This report provides a list of features and their upgrade status, from the last run.<br>Access the detailed feature report through the corresponding link on each feature. |
| `PatchDomain` | `PS1R2UPG.PatchDomain.html` | This report provides details of all domain related changes during the upgrade process.<br>The changes are:<br>■ New EAR or shared libraries deployed during the upgrade process.<br>■ New server resources.<br>■ Foreign JNDI Provider Creation.<br>■ Application of upgrade template for creating the following resources:<br>– New data sources<br>For example:<br>Application DBDS<br>– jrf-async queuesDomain Classpath Upgrade<br>■ OPSS upgrade.<br>■ JRF upgrade. |
| `ROLE_RULE_MEMB` | `PS1R2UPG.ROLE_RULE_MEMB.html` | This report provides details of roles processed on the basis of Search Rule, prepared from Rule Elements, defined in the Rules. |

*Table 6–13 (Cont.) Middle Tier Upgrade Report*

| Feature | Name | Description |
|---|---|---|
| `REQUEST_STAGES` | `PS1R2UPG.REQUEST_STAGES.html` | The following request stages are no longer supported:<br>■ Obtaining Template Approval<br>■ Template Approval Approved<br>■ Template Approval Rejected<br>■ Template Approval Auto Approved<br>This report lists the following:<br>■ Requests for unsupported request stages, processed during upgrade.<br>■ Tasks associated to request with unsupported request stages, processed during upgrade.<br>■ SOA tasks associated to request with unsupported request stages, processed during upgrade. |
| `ReconUpgrade` | `PS1R2UPG.ReconUpgrade.html` | This report lists object names processed during upgrade with names of the associated Horizontal Table Name, Recon Profile Name, and Entity Definition Name. |
| `SOAUpgrade` | NA | New OOTB SOA Composites deployed:<br>■ `sca_DisconnectedProvisioning_rev1.0.jar`<br>■ `sca_DefaultSODApproval_rev1.0.jar` |
| `Scheduler` | NA | This report lists the addition of the following Task Definition's and Scheduler Jobs:<br>■ Account Application Instance Update Task.<br>■ Catalog Synchronization Task.<br>■ Application Instance Post Delete. Processing Task.<br>■ Entitlement Post Delete Processing Task. |
| `ACCESSPOLICY` | `PS12R2UPG.ACCESSPOLICY.html` | This report provides a list of access policy names and the corresponding resource objects, processed during upgrade along with DNLA flag value.<br>Set the value as 1 if DNLA is set, 0 if RNLA is set. |
| `MDSNSUpdate` | NA | Oracle Identity Manager Metadata present in Oracle Identity Manager MDS is updated with the latest namespace to keep them in consoance with changes in XSD Schemas. |
| `OIMConfig` | NA | Oracle Identity Manager Application configuration, kept in the metadata location `/db/oim-config.xml`, is updated as per the latest configuration changes in Oracle Identity Manager 11.1.2. |
| `CONTEXT` | NA | DDL changes in the ORCHPRCESS TABLE.<br>Data from the old context columns (ContextId) is transformed and moved to new context column (ContextVal). |

### 6.4.13 Changing the Deployment Order of Oracle Identity Manager EAR

You must change the deployment order of `oim.ear` from 47 to 48. Complete the following steps to do so:

1. Log in to the WebLogic console.
2. Click **Deployments** in the left pane.
3. Click **oim.ear**.
4. Update the deployment order from 47 to 48, click **Save**.

## 6.4.14 Restarting the Administration Server and SOA Managed Server

To restart the Administration Server and Managed Servers, you must stop them first before starting them again.

To stop the servers, see Shutting Down Administration Server and Managed Servers.

To start the servers, see Starting the Administration Server and SOA Managed Servers.

### Things to Check on the WebLogic Console After Starting the Administration Server

- Check the new data source added:
  1. Log in to Weblogic console.
  2. Click **Data Sources**.
  3. Verify the data source data source given below:

| Name | Type | JNDI Name | Targets |
|---|---|---|---|
| oimApplicationDBDS | Generic | `jdbc/ApplicationDBDS` | `oim_server1` |

- Check for SOA Foreign JNDI provider
  1. Log in to Weblogic console.
  2. Click **Foreign JNDI Providers**.
  3. Verify the existence of Foreign JNDI providers given below:

| Name | Initial Context Factory | Provider URL | User | Targets |
|---|---|---|---|---|
| ForeignJNDIProvider-SOA | weblogic.jndi.WLInitialContextFactory | `t3://celvpint8901.eg.abc.com:<port number>` | WebLogic | `oim_server1` |

- Check the order of the EARs
  1. Log in to Weblogic console.
  2. Click **Deployments**.
  3. Verify the deployment order for the following list respectively:

| Name | State | Health | Type | Deployment Order |
|---|---|---|---|---|
| oim (11.1.1.3.0) | Active | OK | Enterprise Application | 48 |
| OIMAppMetadata (11.1.2.0.0) | Active | OK | Enterprise Application | 47 |

| Name | State | Health | Type | Deployment Order |
|---|---|---|---|---|
| OIMMetadata (11.1.1.3.0) | Active | OK | Enterprise Application | 46 |
| oracle.iam.console.identity.sysadmin.ear (V2.0) | Active | OK | Enterprise Application | 406 |
| oracle.iam.console.identity.self-service.ear (V2.0) | Active | OK | Enterprise Application | 405 |
| oracle.iam.ui.custom(11.1.1,11.1.1) | Active | | Library | 404 |
| oracle.iam.ui.oia-view(11.1.1,11.1.1) | Active | | Library | 403 |
| oracle.iam.ui.view(11.1.1,11.1.1) | Active | | Library | 402 |
| oracle.iam.ui.model(1.0,11.1.1.5.0) | Active | | Library | 401 |

### 6.4.15 Patching Oracle Identity Management MDS Metadata

Oracle Identity Manager 11.1.1.5.0 MDS metadata must be upgraded to Oracle Identity Manager 11.1.2 MDS metadata. Starting the Oracle Identity Manager Managed Servers patches the MDS metadata.

To start the Managed Servers, do the following:

**On UNIX**:

1. Move from your present working directory to the `<MW_HOME>/user_projects/domains/<domain_name>/bin` directory by running the following command on the command line:

   ```
   cd <MW_HOME>/user_projects/domains/<domain_name>/bin
   ```

2. Run the following command to start the Servers:

   ```
   ./startManagedWebLogic.sh <managed_server_name> <admin_url> <user_name>
   <password>
   ```

   where

   `<managed_server_name>` is the name of the Managed Server

   `<admin_url>` is URL of the administration console. Specify it in the format `http://<host>:<port>/console`. Specify only if the WebLogic Administration Server is on a different computer.

   `<user_name>` is the username of the WebLogic Administration Server.

   `<password>` is the password of the WebLogic Administration Server.

**On Windows**:

1. Move from your present working directory to the `<MW_HOME>\user_projects\domains\<domain_name>\bin` directory by running the following command on the command line:

   ```
   cd <MW_HOME>\user_projects\domains\<domain_name>\bin
   ```

2. Run the following command to start the Managed Servers:

   ```
   startManagedWebLogic.cmd <managed_server_name> <admin_url> <user_name>
   <password>
   ```

   where

   `<managed_server_name>` is the name of the Managed Server.

   `<admin_url>` is URL of the administration console. Specify it in the format `http://<host>:<port>/console`. Specify only if the WebLogic Administration Server is on a different computer.

   `<user_name>` is the username of the WebLogic Administration Server.

   `<password>` is the password of the WebLogic Administration Server.

For more information, see "Starting the Stack" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

#### Verifying MDS Patch

Check MDS reports in the following location:

**On UNIX:**

```
<OIM_ORACLE_HOME>/server/logs/MDS_REPORT_DIRECTORY/MDSReport.html
```

**On Windows:**

```
<OIM_ORACLE_HOME>\server\logs\MDS_REPORT_DIRECTORY\MDSReport.html
```

### 6.4.16 Upgrading Oracle Identity Manager Design Console

The Oracle Identity Manager Design Console is used to configure system settings that control the system-wide behavior of Oracle Identity Manager and affect its users. The Design Console allows you to perform user management, resource management, process management, and other administration and development tasks. For more information about the Design Console, see "Design Console Overview" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

Oracle recommends that you install Oracle Identity Manager and the Design Console in different directory paths, regardless of whether the Design Console is on the same system as the Oracle Identity Management server.

To upgrade Design Console, complete the following steps:

1. Back up the following files:

   - On UNIX, `$<XLDC_HOME>/xlclient.sh`
   - `$<XLDC_HOME>/config/xlconfig.xml`
   - On Windows, `<XLDC_HOME>\xlclient.cmd`
   - `<XLDC_HOME>\config\xlconfig.xml`

2. Run the Oracle Identity and Access Management 11.1.2 Installer to upgrade the Design Console home `<XLDC_HOME>`.

   For more information, see "Installing and Configuring Oracle Identity and Access Management (11.1.2)" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

3. Restore the backed up files in the upgraded Design Console home.

4. Build and copy the `wlfullclient.jar` file as follows:

a. Go to `WebLogic_Home/server/lib` directory on UNIX and `WebLogic_Home\server\lib` directory on Windows.

b. Set the `JAVA_HOME` environment variable and add the `JAVA_HOME` variable to the `PATH` environment variable.

   For example, you can set the `JAVA_HOME` to the `jdk160_21` directory inside the Middleware home.

c. Run the following command to build the `wlfullclient.jar` file:

```
java -jar <MW_HOME>/modules/com.bea.core.jarbuilder_1.7.0.0.jar
```

d. Copy the `wlfullclient.jar` file to the `<IAM_HOME>` where you installed the Design Console. For example:

   **On UNIX**:

```
cp wlfullclient.jar <Oracle_IDM2>/designconsole/ext
```

   **On Windows**:

```
copy wlfullclient.jar <Oracle_IDM2>\designconsole\ext
```

## 6.4.17 Upgrading Oracle Identity Manager Remote Manager

Complete the following steps to upgrade Remote Manager:

1. Back up configuration files

   Before starting the Remote Manager upgrade, back up the following Remote Manager configuration files:

   - On UNIX, `$<XLREMOTE_HOME>/remotemanager.sh`
   - `$<XLREMOTE_HOME>/xlremote/config/xlconfig.xml` file.
   - On Windows, `<XLREMOTE_HOME>\remotemanager.bat`
   - `<XLREMOTE_HOME>\xlremote\config\xlconfig.xml` file.

2. Run the Oracle Identity and Access Management Installer to upgrade the Remote Manager home.

   For more information, see "Installing and Configuring Oracle Identity and Access Management (11.1.2)" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

3. Restore configuration files.

   Restore the backed up configuration files in the upgraded Remote Manager home.

## 6.4.18 Configuring BI Publisher Reports

Complete the following steps to configure the BI Publisher Reports:

1. Obtain the reports bundle `oim_product_BIP11gReports_11_1_2_0_0.zip`. from the following location:

   *MW_HOME*/I*AM_HOME*/server/reports/oim_product_BIP11gReports_11_1_2_0_0.zip

2. Unzip `oim_product_BIP11gReports_11_1_2_0_0.zip` at the following location:

   *IAM_HOME*/Middleware/user_projects/domains/*domain_name*/config/bipublisher/repository/Reports/

3. Configure reports by following the instructions in "Configuring Oracle Identity Manager Reports" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

## 6.5 Post-Upgrade Steps

This section contains the following topics:

- After You Upgrade
- Validating the Database Objects
- Creating sysadmin Key
- Impact of Removing Approver-Only Attribute in Request Data Set
- Changes to Request API After Upgrading to Oracle Identity Manager 11g Release 2 (11.1.2)
- Enabling Oracle Identity Manager-Oracle Access Manager Integration After Upgrading to Oracle Identity Manager 11g Release 2 (11.1.2)
- Running the Entitlement List Schedule
- Running the Evaluate User Policies Scheduled Task
- Running Catalog Synchronization
- UMS Notification Provider
- Upgrading User UDF
- Upgrading Application Instances
- Redeploying XIMDD
- Redeploying SPML-DSML
- Customizing Event Handlers
- Upgrading SOA Composites
- Provisioning Oracle Identity Management Login Modules Under WebLogic Server Library Directory
- Authorization Policy Changes
- Verifying the Upgrade

### 6.5.1 After You Upgrade

After upgrading from Oracle Identity Manager 11.1.1.5.0 to Oracle Identity Manager 11.1.2:

- The name of the following EARs remain unchanged from Oracle Identity Manager 11.1.1.5.0 to Oracle Identity Manager 11.1.2:
  - Oracle Identity Manager Metadata (11.1.1.3.0)
  - Oracle Identity Manager (11.1.1.3.0)

  There is no functional loss.
- Resource Object flags are not supported in Oracle Identity Manager 11.1.2. Update all non-system resources with the following values:
  - `Allow All: True`

  - `Provision By Object Admin Only: False`
  - `Self Request Allowed: True`

- All of the resources provisioned to an organization in Oracle Identity Manager 11.1.1.5.0 is available in **Provisioned Accounts,** after upgrading to Oracle Identity Manager 11.1.2. To view, go to the following path:

  1. Connect to the Oracle Identity Manager Identity console.
  2. Go to **Administration**.
  3. Select **Organizations**.
  4. Search for organizations.
  5. Select any organization.
  6. Go to **Provisioned Accounts** to see all Oracle Identity Manager 11.1.1.5.0 based resources, provisioned to an organization.

- In Oracle Identity Manager 11.1.1.5.0, data object permission was shown in the Administration Console under **Roles**.

  In Oracle Identity Manager 11.1.2, data object permission is not shown.

- Oracle Identity Manager 11.1.2 based Oracle Identity Manager reports is supported in BI Publisher 11g.

### 6.5.2 Validating the Database Objects

If you are using Oracle Database, you must check for the `INVALID` schema objects, and compile them if there are any. To do this, complete the following steps:

1. Identify the `INVALID` schema objects by running the following SQL query as `SYS` user:

   ```
   SELECT owner,object_type,object_name,status FROM dba_objects WHERE
   status='INVALID' AND owner in ('<OIM_Schema_Name1>') ORDER BY owner,
   object_type, object_name;
   ```

2. If there are any `INVALID` schema objects, you must compile them by connecting to the database as `SYS` user, and running the following from SQL*Plus:

   ```
   @<$Oracle_Database_Home_Location>/rdbms/admin/utlrp.sql
   ```

   After running the `utlrp.sql`, run the SQL query described in step-1 to ensure that there are no `INVALID` Database objects.

### 6.5.3 Creating sysadmin Key

After you upgrade OIM 11.1.1.5.0 to 11.1.2, you must manually create the `sysadmin` key using Oracle Enterprise Manager console. To do this, complete the following steps:

1. Log in to the Oracle Enterprise Manager console using the following URL:

   ```
   http://<host>:<port>/em
   ```

2. Select **Farm_base_domain**.
3. Expand **WebLogic Domain** on the **Target Navigation** pane.
4. Click **base_domain**.
5. Click on the **WebLogic Domain** drop-down list.

6. Click **Security**, and then click **Credentials**.
7. Select **oracle.wsm.security**.
8. Click **Create Key**.
9. Specify the right values for the following fields:
   - **Select Map**: Select **oracle.wsm.security** for this field.
   - ***Key**: Specify **OIMAdmin**.
   - **Type**: Select **Password**.
   - ***User Name**: Specify the username of the system administrator. For example, `xelsysadm`.
   - ***Password**: Specify the password of the system administrator.
   - ***Confirm Password**: Retype the password to confirm.
10. Click **OK**.

### 6.5.4 Impact of Removing Approver-Only Attribute in Request Data Set

Removing `approver-only` attribute in the Request Data Set results in the following:

- Before upgrade: The requester cannot see attributes `approver-only='true'`, during request submission.

  After upgrade: The requester must provide the value during request submission.

  – All attributes in the request data sets marked with `required=true` and `approver-only=true` should be marked as `required=false` in the data set.

    Make the required fields mandatory in the approver screen through user interface customization.

  – For attributes in the request data sets marked with `required=true`, see Section 6.5.11.2, "User Interface Customization for 11.1.1.5.0 Mandatory UDF and OOTB Attributes" for more information.

- You must manually add LDAP Sync Validation Handler. To do so, complete the following steps:

  1. Export the `EventHandlers.xml` file by running the following WLST offline command:

     **On UNIX:**

     ```
     exportAccessData("/db/ldapMetadata/EventHandlers.xml")
     ```

     **On Windows:**

     ```
     exportAccessData("\\db\\ldapMetadata\\EventHandlers.xml")
     ```

  2. Add the following section of the `EventHandlers.xml` by editing the file in a text editor. Save the file:

     ```
     <validation-handler
     class="oracle.iam.ldapsync.impl.eventhandlers.user.UserCommonNameVa
     lidationHandler" entity-type="User" operation="MODIFY"
     name="UserCommonNameValidationHandler" order="1005" sync="TRUE">

     </validation-handler>

     <validation-handler
     class="oracle.iam.ldapsync.impl.eventhandlers.user.UserCommonNameVa
     ```

```
lidationHandler" entity-type="User" operation="CREATE"
name="UserCommonNameValidationHandler" order="1005" sync="TRUE">
```

```
</validation-handler>
```

3. Import the `EventHandlers.xml` file by running the following WLST offline command:

   **On UNIX:**

   ```
   importAccessData("/db/ldapMetadata/EventHandlers.xml")
   ```

   **On Windows:**

   ```
   importAccessData("\\db\\ldapMetadata\\EventHandlers.xml")
   ```

- You must manually remove the RDN pre-process handler. To do so, complete the following steps:

  1. Export the `EventHandlers.xml` file by running the following WLST offline command:

     **On UNIX:**

     ```
     exportAccessData("/db/ldapMetadata/EventHandlers.xml")
     ```

     **On Windows:**

     ```
     exportAccessData("\\db\\ldapMetadata\\EventHandlers.xml")
     ```

  2. Remove the following section of the `EventHandlers.xml` by editing the file in a text editor. Save the file:

     ```
     <action-handler
     orch-target="oracle.iam.platform.kernel.vo.EntityOrchestration"
     class="oracle.iam.ldapsync.impl.eventhandlers.user.RDNPreProcessHan
     dler" entity-type="User" operation="CREATE"
     name="CreateUserRDNPreProcessHandler" stage="preprocess"
     sync="TRUE" order="10000">
     ```

     ```
     </action-handler>
     ```

     ```
     <action-handler
     orch-target="oracle.iam.platform.kernel.vo.EntityOrchestration"
     class="oracle.iam.ldapsync.impl.eventhandlers.user.RDNPreProcessHan
     dler" entity-type="User"
     operation="MODIFY"name="ModifyUserRDNPreProcessHandler"
     stage="preprocess" sync="TRUE" order="10000">
     ```

     ```
     </action-handler>
     ```

  3. Import the `EventHandlers.xml` file by running the following WLST offline command:

     **On UNIX:**

     ```
     importAccessData("/db/ldapMetadata/EventHandlers.xml")
     ```

     **On Windows:**

     ```
     importAccessData("\\db\\ldapMetadata\\EventHandlers.xml")
     ```

- If you have any custom validation handlers in your environment, ensure that the validation is re-entrant. For more information, see "Writing Custom Validation Event Handlers" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

- If you have any custom user name policy configured in your environment, see "Writing Custom User Name Policy" in the *Oracle Fusion Middleware User's Guide for Oracle Identity Manager* to ensure the following:
  - Use the recommended `oracle.iam.identity.usermgmt.api.UserNameGenerationPolicy` interface to implement policy, instead of using `oracle.iam.identity.usermgmt.api.UserNamePolicy`.
  - Ensure that Custom User Name policy return is the same user login when the approver updates an attribute that does not contribute in generating user login.

## 6.5.5 Changes to Request API After Upgrading to Oracle Identity Manager 11*g* Release 2 (11.1.2)

As part of Oracle Identity Manager 11*g* Release 2 (11.1.2) architecture, changes are introduced to `RequestService` and `UnauthenticatedRequestService` APIs in terms of usage and in terms of concepts involved. Request Template concept is no longer part of Oracle Identity Manager 11*g* Release 2 (11.1.2) and some methods in these APIs are deprecated. Also, `RequestTemplateService` API is completely deprecated.

This section contains the following topics:

- API Methods Deprecated in RequestService
- API Methods Deprecated in UnauthenticatedRequestService
- SELF Request Types Deprecated
- API Methods That Have Changed in Terms of Usage

### 6.5.5.1 API Methods Deprecated in RequestService

The following is a list of API methods deprecated in `RequestService`:

- `public List<String> getTemplateNames()` throws `RequestServiceException`
- `public RequestModel getModelForTemplate(String templateName)` throws `RequestServiceException`
- `public RequestDataSet getRestrictedDataSet(String templateName, String entityType)` throws `RequestServiceException`
- `public RequestTemplate getTemplate(String templateName)` throws `RequestServiceException`
- `public void updateApproverOnlyData(String reqId, List<RequestBeneficiaryEntity> benEntities, List<RequestEntity> reqEntities)` throws `RequestServiceException`
- `public List<String> getTemplateNamesForSelf()` throws `RequestServiceException`
- `public List<RequestTemplate> getRequestTemplates(RequestTemplateSearchCriteria searchCriteria, Set<String> returnAttrs, Map<String,Object> configParams)` throws `RequestServiceException`

The following is a list of API methods deprecated due to storing comments in SOA Human Task comments feature:

- `public void addRequestComment(String reqId, RequestComment comment)` throws `RequestServiceException`
- `public List<RequestComment> getRequestComments(String reqId)` throws `RequestServiceException`
- `public List<RequestComment> getRequestComments(String reqId, RequestComment.TYPE type)` throws `RequestServiceException`
- `public List<RequestComment> getRequestComments(String reqId, String taskId, RequestComment.TYPE type)` throws `RequestServiceException`

### 6.5.5.2 API Methods Deprecated in UnauthenticatedRequestService

The following is a list of API methods deprecated in `UnauthenticatedRequestService`:

- `public List<String> getTemplateNames()` throws `RequestServiceException`
- `public RequestTemplate getTemplate(String templateName)` throws `RequestServiceException`
- `public RequestDataSet getRestrictedDataSet(String templateName, String entitySubType)` throws `RequestServiceException`

### 6.5.5.3 SELF Request Types Deprecated

Request types which were used to perform `SELF` operations have been deprecated. These operations include the following:

- Self Modify User
- Self Assign Roles
- Self Remove Roles
- Self Provision Resource
- Self De-provision Resource
- Self Modify Resource

You can continue with these operations by using the corresponding non-self request types.

### 6.5.5.4 API Methods That Have Changed in Terms of Usage

The only method that have changes in usage is `RequestService.submitRequest()/UnauthenticatedRequestService.submitRequest()`. The API method signature remains the same. However, the way `RequestData` Value Objects are created, have changed. The changes are covered in the following sections:

- Changes to Entity-Type
- Changes to Value Objects
- Code Examples

**6.5.5.4.1 Changes to Entity-Type** Changes to entity-type includes the following:

- `Resource` entity-type is replaced with `Application Instance`.

  Beginning from Oracle Identity Manager 11*g* Release 2 (11.1.2), in order to create any provision, revoke, disable, and enable account type of request, the `entityType` property must be set to `ApplicationInstance` instead of `Resource`.

- A new entity-type called Entitlement is introduced in Oracle Identity Manager 11*g* Release 2 (11.1.2). Oracle Identity Manager supports creating Provision Entitlement and Revoke Entitlement type of requests.

#### 6.5.5.4.2 Changes to Value Objects

Changes to value objects, related to RequestData includes the following:

- requestTemplateName property which was a part of oracle.iam.request.vo.RequestData value objects is deprecated. Even if you set this property, it is not honoured.
- A new property called operation is introduced in oracle.iam.request.vo.RequestEntity and oracle.iam.request.vo.RequestBeneficiaryEntity value objects. It is mandatory to set this property while creating the value objects. You can use the following constants defined in oracle.iam.request.vo.RequestConstants class.
  - MODEL_CREATE_OPERATION – Create User operation
  - MODEL_MODIFY_OPERATION – Modify User operation
  - MODEL_DELETE_OPERATION – Delete User operation
  - MODEL_ENABLE_OPERATION – Enable User operation
  - MODEL_DISABLE_OPERATION – Disable User operation
  - MODEL_ASSIGN_ROLES_OPERATION – Assign Roles operation
  - MODEL_REMOVE_ROLES_OPERATION – Remove Roles operation
  - MODEL_PROVISION_APPLICATION_INSTANCE_OPERATION – Provision Application Instance operation
  - MODEL_MODIFY_ACCOUNT_OPERATION – Modify Account operation
  - MODEL_REVOKE_ACCOUNT_OPERATION – Revoke Account operation
  - MODEL_ENABLE_ACCOUNT_OPERATION – Enable Account operation
  - MODEL_DISABLE_ACCOUNT_OPERATION – Disable Account operation
  - MODEL_PROVISION_ENTITLEMENT_OPERATION – Provision Entitlement operation
  - MODEL_REVOKE_ENTITLEMENT_OPERATION – Revoke Entitlement operation
  - MODEL_ACCESS_POLICY_PROVISION_APPINSANCE_OPERATION – Access Policy based provisioning operation
- While creating RequestEntity or RequestBeneficiaryEntity value objects, you can also use the following method to set the entityType property:

  ```
  public void setRequestEntityType(oracle.iam.platform.utils.vo.OIMType
  type)
  ```

  ```
  type - OIMType.Role/ OIMType.ApplicationInstance/OIMType.Entitlement/
  OIMType.User
  ```

#### 6.5.5.4.3 Code Examples

Listed below are some code examples:

- Create a RequestData for a Create User operation as follows:

  ```
  RequestData requestData = new RequestData("Create User");
  requestData.setJustification("Creating User John Doe");
  String usr = "John Doe";

  RequestEntity ent = new RequestEntity();
  ```

```
ent.setEntityType(RequestConstants.USER);
ent.setOperation(RequestConstants.MODEL_CREATE_OPERATION); //New in R2
List<RequestEntityAttribute> attrs = new ArrayList<RequestEntityAttribute>();

RequestEntityAttribute attr = new RequestEntityAttribute("Last Name", usr,
RequestEntityAttribute.TYPE.String);
attrs.add(attr);
attr = new RequestEntityAttribute("First Name", usr,
RequestEntityAttribute.TYPE.String);
attrs.add(attr);
attr = new RequestEntityAttribute("User Login", usr,
RequestEntityAttribute.TYPE.String);
attrs.add(attr);
attr = new RequestEntityAttribute("Password", "Welcome123",
RequestEntityAttribute.TYPE.String);
attrs.add(attr);
attr = new RequestEntityAttribute("Organization", 1L,
RequestEntityAttribute.TYPE.Long);
attrs.add(attr);
attr = new RequestEntityAttribute("User Type", false,
RequestEntityAttribute.TYPE.Boolean);
attrs.add(attr);
attr = new RequestEntityAttribute("Role", "Full-Time",
RequestEntityAttribute.TYPE.String);
attrs.add(attr);
ent.setEntityData(attrs);

List<RequestEntity> entities = new ArrayList<RequestEntity>();
entities.add(ent);
requestData.setTargetEntities(entities);

//Submit the request with the above requestData
```

- Create a `RequestData` for an Assign Roles operation as follows:

```
RequestData requestData = new RequestData();

requestData.setJustification("Assigning IDC ADMIN Role(role key 201) to user
with key 121");

RequestBeneficiaryEntity ent1 = new RequestBeneficiaryEntity();
ent1. setRequestEntityType (oracle.iam.platform.utils.vo.OIMType.Role);
ent1.setOperation(oracle.iam.request.vo.RequestConstants.MODEL_ASSIGN_ROLES_
OPERATION); //New in R2
ent1.setEntitySubType("IDC ADMIN");
ent1.setEntityKey("201");

List<RequestBeneficiaryEntity> entities = new
ArrayList<RequestBeneficiaryEntity>();
entities.add(ent1);

Beneficiary beneficiary = new Beneficiary();
beneficiary.setBeneficiaryKey("121");
beneficiary.setBeneficiaryType (Beneficiary.USER_BENEFICIARY);
beneficiary.setTargetEntities(entities);

List<Beneficiary> beneficiaries = new ArrayList<Beneficiary>();
beneficiaries.add(beneficiary);
requestData.setBeneficiaries(beneficiaries);

//Submit the request with the above requestData
```

- Create a `RequestData` for a Provision Application Instance operation as follows:

```
RequestData requestData = new RequestData();

requestData.setJustification("Creating AD User (app instance key 201) account
to user with key 121");

RequestBeneficiaryEntity ent1 = new RequestBeneficiaryEntity();
ent1. setRequestEntityType
(oracle.iam.platform.utils.vo.OIMType.ApplicationInstance);
ent1.setOperation(oracle.iam.request.vo.RequestConstants.MODEL_PROVISION_
APPLICATION_INSTANCE_OPERATION);
ent1.setEntitySubType("AD User");
ent1.setEntityKey("201");

List<RequestBeneficiaryEntityAttribute> attrs = new
ArrayList<RequestBeneficiaryEntityAttribute>();
//Update 'attrs' above with all the data specific to AD User form.
ent1.setEntityData(attrs);

List<RequestBeneficiaryEntity> entities = new
ArrayList<RequestBeneficiaryEntity>();
entities.add(ent1);

Beneficiary beneficiary = new Beneficiary();
beneficiary.setBeneficiaryKey("121");
beneficiary.setBeneficiaryType(Beneficiary.USER_BENEFICIARY);
beneficiary.setTargetEntities(entities);

List<Beneficiary> beneficiaries = new ArrayList<Beneficiary>();
beneficiaries.add(beneficiary);
requestData.setBeneficiaries(beneficiaries);
//Submit the request with the above requestData
```

- Create a `RequestData` for a Provision Entitlement operation as follows:

```
RequestData requestData = new RequestData();
Beneficiary beneficiary1 = new Beneficiary();
beneficiary1.setBeneficiaryKey("222");
beneficiary1.setBeneficiaryType(Beneficiary.USER_BENEFICIARY);

RequestBeneficiaryEntity ent1 = new RequestBeneficiaryEntity();
ent1.setEntityType(RequestConstants.ENTITLEMENT);
ent1.setEntitySubType("AD USER ENTITLEMENT1");
ent1.setEntityKey("122");
ent1.setOperation(RequestConstants.MODEL_PROVISION_ENTITLEMENT_OPERATION);

List<RequestBeneficiaryEntity> entities1 = new
ArrayList<RequestBeneficiaryEntity>();
entities1.add(ent1);
beneficiary1.setTargetEntities(entities1);

List<Beneficiary> beneficiaries = new ArrayList<Beneficiary>();
beneficiaries.add(beneficiary1);
requestData.setBeneficiaries(beneficiaries);
//Submit the request with the above requestData
```

## 6.5.6 Enabling Oracle Identity Manager-Oracle Access Manager Integration After Upgrading to Oracle Identity Manager 11*g* Release 2 (11.1.2)

> **Note:** Perform this task only if you want to integrate Oracle Identity Manager with Oracle Access Manager for single sign-on, after upgrading to Oracle Identity Manager 11.1.2.
>
> Ensure that Oracle Access Manager is at release 11.1.1.5.2 or later.

If you want to integrate Oracle Identity Manager 11.1.2 with Oracle Access Manager for single sign-on, then you must upgrade Oracle Access Manager to 11.1.1.5.2 or later. If your Oracle Access Manager version is less than 11.1.1.5.2, the auto-login functionality does not work.

After upgrading to Oracle Identity Manager 11.1.2, upgrade Oracle Identity Manager and Oracle Access Manager configurations for auto-login functionality to work. After upgrading the configurations, NAP protocol is replaced by TAP protocol for communication between Oracle Identity Manager and Oracle Access Manager.

The following topics provide upgrade instructions for two possible scenarios:

- Using 10g WebGate for Oracle Identity Manager-Oracle Access Manager Integration
- Using 11g WebGate for Oracle Identity Manager-Oracle Access Manager Integration

Before you begin with the upgrade configuration procedures, refer to the "Using the idmConfigTool Command" for more about the **IdmConfigTool** in the *Oracle Fusion Middleware Integration Guide for Oracle Identity Management Suite*.

### 6.5.6.1 Using 10*g* WebGate for Oracle Identity Manager-Oracle Access Manager Integration

If you are using 10*g* WebGate, complete the following steps to upgrade Oracle Identity Manager and Oracle Access Manager configurations:

1. In the **idmConfigTool**, run `configOAM`. This creates a 10*g* WebGate agent and an 11*g* WebGate agent in Oracle Access Manager. Ensure that the artifacts corresponding to both WebGates are created in `<DOMAIN_HOME>/output directory`.
2. In the **idmConfigTool**, run `configOIM`. In a cross-domain setup where Oracle Identity Manager and Oracle Access Manager are in two different WebLogic domains, specify the following additional properties before running this option:
   - `OAM11G_WLS_ADMIN_HOST: <host name of OAM admin server machine>`
   - `OAM11G_WLS_ADMIN_PORT: <OAM admin server port>`
   - `OAM11G_WLS_ADMIN_USER: <admin user of OAM domain>`

   > **Note:** When running the `configOIM` option, ensure that you provide the same properties that you provided in the `configOAM` option for `OAM_TRANSFER_MODE` and `ACCESS_GATE_ID` properties.
   >
   > The `WEBGATE_TYPE` property should be specified as `ohsWebgate10g`.

3. Restart the Administration and Managed Servers. In the case of a cross domain setup, restart servers from both the domains.

   Restart the Oracle Identity Manager Administration Server and Managed server as follows:

   **On UNIX:**

   ```
   <MW_HOME>/user_projects/domains/domain_name/startWebLogic.sh
   ```

   ```
   <MW_HOME>/user_projects/domains/domain_
   name/bin/startManagedWebLogic.sh <managed_server1>
   ```

   **On Windows:**

   ```
   <MW_HOME>\user_projects\domains\domain_name\startWebLogic.cmd
   ```

   ```
   MW_HOME\user_projects\domains\domain_name\bin\startManagedWebLogic.cmd
   <oim_server>
   ```

   For more information, see "Restarting Servers" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

### 6.5.6.2 Using 11*g* WebGate for Oracle Identity Manager-Oracle Access Manager Integration

If you are using 11*g* WebGate, complete the following steps to upgrade Oracle Identity Manager and Oracle Access Manager configurations:

1. In the **idmConfigTool**, run `configOAM`. This creates a 10*g* WebGate agent and an 11*g* WebGate agent in Oracle Access Manager. Ensure that the artifacts corresponding to both WebGates are created in the `<DOMAIN_HOME>/output directory`.

2. In the **idmConfigTool**, run `configOIM`. In cross-domain setup where Oracle Identity Manager and Oracle Access Manager are in two different WebLogic domains, specify the following additional properties before running this option:

   - `OAM11G_WLS_ADMIN_HOST: <host name of OAM admin server machine>`
   - `OAM11G_WLS_ADMIN_PORT: <OAM admin server port>`
   - `OAM11G_WLS_ADMIN_USER: <admin user of OAM domain>`

   > **Note:** When running the `configOIM` option, ensure that you provide the same properties that you provided in the `configOAM` option for `OAM_TRANSFER_MODE` and `ACCESS_GATE_ID` properties.
   >
   > The `WEBGATE_TYPE` property should be specified as `ohsWebgate11g`.

3. Restart the Administration and Managed servers. In the case of a cross domain setup, restart servers from both the domains.

   Restart the Oracle Identity Manager Administration Server and Managed server as follows:

   **On UNIX:**

   ```
   <MW_HOME>/user_projects/domains/domain_name/startWebLogic.sh
   ```

   ```
   <MW_HOME>/user_projects/domains/domain_
   name/bin/startManagedWebLogic.sh <managed_server1>
   ```

   **On Windows:**

```
<MW_HOME>\user_projects\domains\domain_name\startWebLogic.cmd
```

```
MW_HOME\user_projects\domains\domain_name\bin\startManagedWebLogic.cmd
<oim_server>
```

For more information, see "Restarting Servers" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

### 6.5.7 Running the Entitlement List Schedule

You must run the Entitlement List Schedule task in order to use catalog features.

Complete the following steps to run the Entitlement List Schedule job:

1. Log in to the following location:

   `http://<OIM_HOST>:<OIM_PORT>/sysadmin`

2. Click **System Management**.
3. Select **Scheduler**.
4. Enter "Entitlement List" in the **Search Scheduled Jobs** field and click **Search**.
5. Select **Entitlement List**.
6. Click **Run Now**. Wait till the job is complete.

### 6.5.8 Running the Evaluate User Policies Scheduled Task

You must run the Evaluate User Policies scheduled task to start provisioning based on access policy after the role grant. This scheduled task can be configured to run every 10 minutes, or you can run this scheduled task manually.

To start the scheduler, see "Starting and Stopping the Scheduler" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.

### 6.5.9 Running Catalog Synchronization

Resource objects are transformed during the upgrade process. In order to provision the resource of an object, called App instance, with Oracle Identity Manager 11.1.2, you must run the Catalog Synchronization job.

For more information, see "Bootstrapping the Catalog" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.

> **Note:** If no Entitlements show up, make sure that the entitlements field in the child tables is set to `Entitlement=true` and reloaded into the parent form.

### 6.5.10 UMS Notification Provider

This is a new Oracle Identity Manager 11.1.2 feature for notification. If you want to use this new notification model, after upgrading to 11.1.2, complete the following steps:

1. Configure Email driver from Enterprise Manager user interface:

   a. Log in to Oracle Enterprise Manager Fusion Middleware Control and do the following:

      i. Expand **Application Deployments**.

      ii. Expand **User Messaging Service**.

iii. Select **usermessagingdriver-email (<soa_server1>)**.

iv. Select **Email Driver Properties**.

v. Select **in Driver-Specific Configuration**.

**b.** Configure the values, as listed in Table 6–14:

*Table 6–14 UMS Parameters and Description*

| Parameter | Description |
|---|---|
| OutgoingMailServer | Name of the SMTP server.<br>For example:<br>`abc.example.com` |
| OutgoingMailServerPort | Port of the SMTP server.<br>For example:<br>456 |
| OutgoingMailServerSecurity | The security setting used by the SMTP server Possible values can be None/TLS/SSL. |
| OutgoingUsername | Provide a valid username.<br>For example:<br>`abc.eg@example.com` |
| OutgoingPassword | Complete the following:<br>**1.** Select **Indirect Password**. Create a new user.<br>**2.** Provide a unique string for indirect **Username/Key**.<br>For example:<br>`OIMEmailConfig`. This mask the password and prevent it from exposing it in cleartext, in the config file.<br>**3.** Provide valid password for this account. |

**2.** Configure the Notification provider XML through the Enterprise Manager user interface:

**a.** Log in to Enterprise Manager and do the following:

i. Expand **Application Deployments**.

ii. Select **OIMAppMetadata(11.1.1.3.0)(oim_server1)** and right-click.

iii. Select **System MBean Browser**.

iv. Expand **Application Defined MBeans**.

v. Expand **oracle.iam**.

vi. Expand **Server_OIM_Server1**

vii. Expand **Application: oim**.

viii. Expand **IAMAppRuntimeMBean**.

ix. Select **UMSEmailNotificationProviderMBean**.

**b.** Configure the values, as listed in Table 6–15:

*Table 6–15 Parameter for Configuring Notification Provider*

| Parameter | Description |
|---|---|
| Web service URL | Start the URL of UMS web service. Any SOA server can be used.<br>For example:<br>`http://<SOA_host>:<SOA_Port>/ucs/messaging/webservice` |
| Policies | The OWSM Policy is attached to the given web service, leave it blank. |
| Username | The username is given in the security header of web service. If there is no policy attached, leave it blank. |
| Password | The password given in the security header of web service. If there is no policy attached, leave it blank. |

After upgrading to 11.1.2, if you want to use SMTP notification provider instead of the default UMS notification provider, do the following:

1. Log in to Enterprise Manager and do the following:
   a. Expand **Application Deployments**.
   b. Select **OIMAppMetadata(11.1.1.3.0)(oim_server1)** and Right click.
   c. Select **System MBean Browser**.
   d. Expand **Application Defined MBeans**.
   e. Expand **oracle.iam**.
   f. Expand **Server_OIM_Server1**
   g. Expand **Application: oim**.
   h. Expand **IAMAppRuntimeMBean**.
   i. Select **UMSEmailNotificationProviderMBean**.
2. Ensure that the value of the attribute `Enabled` is set to `true`.
3. Provide the configuration values in MBean (username, password, mailServerName) or the name of IT Resource in MBean.

   The IT Resource name is the name given in `XL.MailServer` system property, before you upgrade Oracle Identity Manager 11.1.1.5.0 to Oracle Identity Manager 11.1.2.

## 6.5.11 Upgrading User UDF

You must have UDF in your environment because if you do not update your User Interface with UDFs, several features like user creation, role creation, and self registration request where UDFs are involved fails.

This section contains the following topics:

- Rendering the UDFs
- User Interface Customization for 11.1.1.5.0 Mandatory UDF and OOTB Attributes
- Lookup Query Modification

#### 6.5.11.1 Rendering the UDFs

For an Oracle Identity Manager 11.1.2 environment that has been upgraded from Oracle Identity Manager 11.1.1.5.0, the custom attributes for user entity already exist in the back-end. These attributes are not present as form fields on the Oracle Identity Manager 11.1.2 user interface screens until the user screens are customized to add the custom fields.

However, before you can customize the screens, you must first complete upgrading the custom attributes using the Upgrade User Form link in the System Administration console.

After completing the Upgrade User Form, the User value object (VO) instances in various Data Components like DataComponent-Catalog, DataComponent-My Information, DataComponent-User Registration shows the custom attributes. This includes all custom attributes available for Web Composer (Customized) and can be added to User user interface screens.

For more information, see "Customizing the Interface" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

Complete the following steps to render UDFs:

1. Log in to the **Identity System Administration** console.
2. Click **Sandboxes**. Click **Create Sandbox**. A Create Sandbox window appears.
3. Enter the **Sandbox Name**. Select **Activate Sandbox**. Click **Save and Close**.
4. Go to **Upgrade**. Select **Upgrade User Form**. Click **Upgrade Now**.
5. Publish the Sandbox.
6. Log out from Identity System Administration console.
7. Log in to **Identity Self Service** console.
8. Click **Create Sandbox**. A **Create Sandbox** window appears.
9. Enter the **Sandbox Name**. Select **Activate Sandbox**. Click **Save and Close**.
10. From the left navigation pane, select **Users**.
11. Click **Create User**. A **Create User** page opens. Fill up all the mandatory fields. Add the same UDFs in **Modify User** and **User Detail** screen. Select the correct **Data Component** and **UserVO Name** as listed in Table 6–16.

    For example:

    From the left navigation pane, click **Users**. Click **User** to go to the **Create User** screen and fill all mandatory fields.
12. Click **Customize** on top right. Select **View**. Select **Source**.
13. Select **Name** in **Basic Information** and click **Edit** on the confirmation window.
14. Select **panelFormLayout**. Click **Add Content**.
15. Select the correct **Data Component** and **VO Name** as listed in Table 6–16:

*Table 6–16 UDF Screens and Description*

| Screen Name | Data Component | VO Name | Procedure |
|---|---|---|---|
| Create User | Data Component - Catalog | UserVO | Do the following:<br>1. Click **User**.<br>2. Click **Create**, it launches the **Create User** screen. |
| Modify User | Data Component - Catalog | UserVO | Do the following:<br>1. Click **User** and search.<br>2. Select a single user from search results.<br>3. Click **Edit**, it launches the **Modify User** screen. |
| View User Details | Data Component - Manage Users | UserVO1 | Do the following:<br>1. Click **User** and search.<br>2. Select a single user from search results. |
| Bulk Modify User Flow | Data Component - Catalog | UserVO | Do the following:<br>1. Click **User** and search.<br>2. Select more than a single user from search results. |
| My Information | Data Component - My Information | UserVO1 | Do the following:<br>1. Click **Identity**.<br>2. Select the **My Information** sub-tab. |
| Customizing Search Results | Data Component - Manage Users | UserVO1 | Do the following:<br>1. Click **Identity**.<br>2. Click **Users**.<br>3. Click **Customizations**, it opens the **Web Composer**. |
| User Registration | Data Component - User Registration | UserVO1 | Do the following:<br>1. Click **Customize** to open **Web Composer**.<br>2. Enable the left navigation links for unauthenticated pages.<br>3. Click **User Registration**.<br>4. Select **User Registration**. |
| Adding UDF in Search Panel | NA | NA | Do the following:<br>1. Log in to Identity<br>2. Click **User**.<br>3. Search for "Add Fields" in the search box. It shows all searchable fields to the user. |
| Customizing Request Summary/Details | NA | NA | Requests created after Create User, Modify User, My Information, Self Registration |

16. Click **Close**.
17. Click **Sandboxes**. Export the sandbox using **Export Sandbox.**
18. Publish the sandbox.
19. Log out from **Identity Self Service**, and log in again. The added UDF in the screen is seen.

#### 6.5.11.2 User Interface Customization for 11.1.1.5.0 Mandatory UDF and OOTB Attributes

If you have rendered the OOTB attributes as mandatory in Oracle Identity Manager 11.1.1.5.0, you must customize the user interface in order to achieve the same customizations after upgrade.

1. Log in to **Identity System Administration** console.
2. Click **Sandboxes**. Click **Create Sandbox**. A Create Sandbox window appears.
3. Enter the **Sandbox Name**. Select **Activate Sandbox**. Click **Save and Close**.
4. Go to **Upgrade**. Select **Upgrade User Form**. Click **Upgrade Now**.
5. Publish the Sandbox.
6. Log out from Identity System Administration console.
7. Log in to **Identity Self Service** console.
8. Click **Create Sandbox**. A **Create Sandbox** window appears.
9. Enter the **Sandbox Name**. Select **Activate Sandbox**. Click **Save and Close**.
10. From the left navigation pane, click **Users**. Click **User** to go to the **Create User** screen and fill all the mandatory fields.
11. Click **Customize** on top right. Select **View**. Select **Source**.
12. Select **Name** in **Basic Information** and click **Edit** on the confirmation window.
13. Select **panelFormLayout**. Click **Add Content**.
14. Click **Input Component** and click **Edit**.
15. On the Component Properties dialogue, select **Show Required** checkbox. In the Required field, select **Expression Editor**, and in the **Expression Editor** field, enter the value as **true**.
16. Click **Close**.
17. Click **Sandboxes**. Export the sandbox using **Export Sandbox.**
18. Publish the sandbox.
19. Log out from **Identity Self Service**, and log in again. The added UDF on the screen with an asterix (*) symbol is seen.

#### 6.5.11.3 Lookup Query Modification

In user customization upgrade, multiple values for the Save Column may exist in `User.xml`. Based on the possible values; single, multiple, and null, do the following in the upgraded environment:

- Use `Single` value for Save Column: User creation is successful, and the value of the field is also saved in database.

- Use `Multiple` or `NULL` value for Save Column: User creation is successful, but the value is not saved in database.

#### Recommendation

Update the **Lookup By Query** metadata definition attached to an attribute in User or Role through Config Service or Design Console.

For more information, see Section 6.4.16, "Upgrading Oracle Identity Manager Design Console".

> **Note:** You can customize Role UDF and Organization UDF, as done in Section 6.5.11, "Upgrading User UDF".

### 6.5.12 Upgrading Application Instances

After you complete the upgrade, you must complete the following steps to upgrade Application Instances:

1. Log in to the following console:

   ```
   http://<OIM_HOST>:<OIM_PORT>/sysadmin
   ```

2. Expand **Upgrade** on the left navigation pane.
3. Click **Upgrade Application Instances**.

This creates the U/I Forms and Datasets for the Application Instances, and seeds to MDS.

### 6.5.13 Redeploying XIMDD

> **Note:** This section is required only if the Diagnostic Dashboard services for AD Password Sync were deployed in 11.1.1.5.0 and if your application is deployed in staging mode in 11.1.1.5.0.

Before you can re-deploy, you must undeploy XIMDD from the 11.1.1.5.0 Oracle Identity Manager Managed Server or from the cluster. To do so, complete the following steps:

1. Log in to the WebLogic Server Administration console:

   ```
   host:admin port/console
   ```

2. If you are running in production mode, click **Lock and Edit**.
3. Click **Deployments**.
4. In the resulting list, look for **XIMDD**.
5. If they are running, select **XIMDD.**
6. Click **Delete**.
7. Activate the changes.

To redeploy, complete the following steps:

1. Log in to the WebLogic Server Administration console:

   ```
   host:admin port/console
   ```

2. Click **Lock & Edit**.
3. Click **Deployments**.
4. Click **Install**.
5. In the path, give the path for XIMDD.ear

   The default path is in the following location:

   On UNIX, `$<OIM_HOME>/server/webapp/optional`

   On Windows, `<OIM_HOME>\server\webapp\optional`
6. Select **XIMDD.ear**. Click **Next**.
7. Select **Install this deployment as an application**. Click **Next** .
8. In **Select deployment targets** page, select **oim server**. Click **Next**.
9. In the **Optional Setting** page, click **Finish**.
10. Click **Deployments**.
11. Select **XIMDD**. Click **Start**.
12. From the options, select **Service All Requests**.

### 6.5.14 Redeploying SPML-DSML

**Note:** This section is required only if the DSML web services for AD Password Sync were deployed in 11.1.1.5.0.

Before you can redeploy, you must undeploy SPML-DSML from the 11.1.1.5.0 Oracle Identity Manager Managed Server or from the cluster. To do so, complete the following steps:

1. Log in to the WebLogic Server Administration console:

   ```
   host:admin port/console
   ```
2. If you are running in production mode, obtain the Lock in order to make updates.
3. Click **Deployments**.
4. In the resulting list, look for **spml**.
5. If they are running, select **spml.**
6. Click **Delete**.
7. Activate the changes.

To redeploy, complete the following steps:

1. Log in to WebLogic Server Administration console through the following path:

   host:admin port/console
2. Click **Lock & Edit**.
3. Click **Deployments**.
4. Click **Install**.
5. In the path give the path for spml.ear

   The default path is in the following location:

On UNIX, `$<OIM_HOME>/server/webapp/optional`

On Windows, `<OIM_HOME>\server\webapp\optional`

6. Select **spml.ear**. Click **Next**.
7. Select **Install this deployment as an application**. Click **Next** .
8. In **Select deployment targets** page, select **oim server**. Click **Next**.
9. In the **Optional Setting** page, click **Finish**.
10. Click **Deployments**.
11. Select **spml**. Click **Start**.
12. From the options, select **Service All Requests**.

## 6.5.15 Customizing Event Handlers

If you have used any event handlers in Oracle Identity Manager 11.1.1.5.0, you must re-customize the event handler for Oracle Identity Manager 11.1.2.

For more information, see "Developing Custom Event Handlers" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

## 6.5.16 Upgrading SOA Composites

You must manually upgrade OOTB composites and custom composites built before upgrading to 11.1.2.

This section contains the following topics:

- OOTB Composites Not Modified Before Upgrading
- OOTB Composites Modified Before Upgrading And Custom Composites

> **Note:** Redeploying a composite moves all pending tasks to `STALE` state. Oracle recommends you to close any pending task before upgrading the composites.

### 6.5.16.1 OOTB Composites Not Modified Before Upgrading

Upgrade OOTB composites that are not modified, using either JDeveloper or SOA Composer, before upgrading to Oracle Identity Manager 11.1.2. Complete the following steps to upgrade `DefaultRequestApproval` composite:

1. Move from your present working directory to the `<OIM_ORACLE_HOME>/server/workflows` directory by running the following command on the command line:

   **On UNIX:**

   ```
   cd <OIM_ORACLE_HOME>/server/workflows
   ```

   **On Windows**:

   ```
   cd <OIM_ORACLE_HOME>\server\workflows
   ```

2. Unzip `DefaultRequestApproval.zip`.
3. Log in to the Oracle Enterprise Manager console:

   ```
   http://<host>:<port>/em
   ```

4. Expand **Farm_<oim_domain_name>_d > SOA -> soa-infra -> default**
5. Right click **DefaultRequestApproval[1.0]** and select **SOA Deployment -> Redeploy**
6. Select **Archive is on the machine where Enterprise Manager is running**.
7. Provide the absolute path to the `sca` jar for `DefaultRequestApproval` composite:

   **On UNIX**:

   ```
   <OIM_
   HOME>/server/workflows/composites/DefaultRequestApproval/deploy/sca_
   DefaultRequestApproval_rev1.0.jar
   ```

   **On Windows:**

   ```
   <OIM_
   HOME>server\workflows\composites\DefaultRequestApproval\deploy\sca_
   DefaultRequestApproval_rev1.0.jar
   ```

8. Select **No Configuration plan is required**.
9. Click **Next**.
10. Select **Deploy as default revision**.
11. Click **Redeploy**.

Repeat steps 2 to 11 for the remaining composites, which were not modified before upgrading to Oracle Identity Manager 11.1.2.

> **Note:** `DefaultResourceAuthorizer` and `DefaultResourceAdministrator` are no longer supported in 11.1.2.

### 6.5.16.2 OOTB Composites Modified Before Upgrading And Custom Composites

Upgrade custom composites created before upgrading to Oracle Identity Manager 11.1.2 and OOTB composites modified, using either JDeveloper or SOA Composer, before upgrading to Oracle Identity Manager 11.1.2. Complete the following steps to upgrade `DefaultRequestApproval` composite:

1. Open the SOA composite project in JDeveloper (Use Jdeveloper 11.1.1.6.0).
2. Open `ApprovalTask.task` file in designer mode.
3. Select **General**.
4. Change **Owner** to **Group, SYSTEM ADMINISTRATORS, STATIC**.
5. Select **Outcomes lookup**. An **Outcomes Dialog** opens.
6. Select **Outcomes Requiring Comment**.
7. Select **Reject** and click **Ok**.
8. Click **Ok** again.
9. Select **Notification**.
10. Click on the update icon under **Notification**. Update any old URLs in notification with the corresponding new URL in 11.1.2. An example notification content is given below:

    ```
    A <%/task:task/task:payload/task:RequestModel%> request has been assigned to
    you for approval. <BR><BR>
    ```

```
Request ID: <%/task:task/task:payload/task:RequestID%> <BR>
Request type: <%/task:task/task:payload/task:RequestModel%> <BR>
<BR>
Access this task in the
<A
style="text-decoration: none;"
href=<%substring-before(/task:task/task:payload/task:url,
"/workflowservice/CallbackService")%>/identity/faces/home?tf=approval_details
>
Identity Self Service
</A>
 application or take direct action using the links below. Approvers are
required to provide a justification when rejecting the request
```

11. Click **Advanced**.
12. Deselect **Show worklist/workspace URL in notifications**. Provide the URL to Pending Approvals in identity application as shown in the example in step 10.
13. Repeat step 1 to 12 for other human tasks, if any, in the composite. Save your work.
14. Right click **Project** and select **Deploy -> Deploy to Application Server**.
15. Provide revision ID. Select **Mark revision as default** and **Overwrite any existing composite with same revision ID**.

> **Note:** You can also deploy the composites with different revision ID. In that case you have to modify all approval policies using this composite.

16. Select your application server connection, if it already exists, and click **Next**. Create an application server connection if it does not exist.
17. Click **Next**.
18. Click **Finish**.

Repeat the procedure for the remaining custom composites and modified OOTB composites as well.

### 6.5.17 Provisioning Oracle Identity Management Login Modules Under WebLogic Server Library Directory

> **Note:** This task is required only if `OIMAuthenticator.jar` is already present under the `<MW_HOME>/wlserver_10.3/server/lib/mbeantypes` directory.

Apply the following steps across all the WebLogic Server homes in the domain :

**On UNIX:**

1. Copy `OIMAuthenticator.jar`, `oimmbean.jar`, `oimsigmbean.jar`, and `oimsignaturembean.jar` files located under `<OIM_ORACLE_HOME>/server/loginmodule/wls` directory to `<MW_HOME>/wlserver_10.3/server/lib/mbeantypes` directory by running the following command on the command line:

```
cp <OIM_ORACLE_HOME>/server/loginmodule/wls/* <MW_HOME>/wlserver_
10.3/server/lib/mbeantypes/
```

2. Move from your present working directory to the `<MW_HOME>/wlserver_10.3/server/lib/mbeantypes` directory by running the following command on the command line:

   ```
   cd <MW_HOME>/wlserver_10.3/server/lib/mbeantypes
   ```

3. Change the permissions on these files to 750 by using the `chmod` command:

   ```
   chmod 750 *
   ```

4. Restart all servers in the domain.

**On Windows:**

1. Copy `OIMAuthenticator.jar`, `oimmbean.jar`, `oimsigmbean.jar`, and `oimsignaturembean.jar` files located under `<OIM_ORACLE_HOME>\server\loginmodule\wls` directory to `<MW_HOME>\wlserver_10.3\server\lib\mbeantypes` directory by running the following command on the command line:

   ```
   cp <OIM_ORACLE_HOME>\server\loginmodule\wls\* <MW_HOME>\wlserver_
   10.3\server\lib\mbeantypes
   ```

2. Move from your present working directory to the `<MW_HOME>\wlserver_10.3\server\lib\mbeantypes` directory by running the following command on the command line:

   ```
   cd <MW_HOME>\wlserver_10.3\server\lib\mbeantypes
   ```

3. Change the permissions on these files to 750 by using the `chmod` command:

   ```
   chmod 750 *
   ```

4. Restart all servers in the domain.

### 6.5.18 Authorization Policy Changes

If you have custom Authorization Policies in Oracle Identity Manager in 11*g* Release 1 (11.1.1.5.0), in order to create or modify users, you must assign new administrator roles in relation to User Administration, Role Administration, or Help Desk.

Table 6–17 lists the Administration roles in Oracle Identity Manager 11g, either removed or consolidated into the System Administrator Administration role for all system administrative operations in Oracle Identity Manager 11.1.2:

***Table 6–17 Changes in Role from Oracle Identity Manager 11g to 11.1.2***

| Sl No. | Roles in Oracle Identity Manager 11*g* | Roles Removed and Replaced in Oracle Identity Manager 11.1.2 |
|---|---|---|
| 1 | SCHEDULER ADMINISTRATORS | Removed and replaced with SYSTEM CONFIGURATORS. |
| 2 | DEPLOYMENT MANAGER ADMINISTRATORS | Removed and replaced with SYSTEM CONFIGURATORS. |
| 3 | NOTIFICATION TEMPLATE ADMINISTRATORS | Removed and replaced with SYSTEM CONFIGURATORS. |
| 4 | SOD ADMINISTRATORS | Removed and replaced with SYSTEM ADMINISTRATORS. |
| 5 | SYSTEM CONFIGURATION ADMINISTRATORS | Removed and replaced with SYSTEM CONFIGURATORS. |

*Table 6–17 (Cont.) Changes in Role from Oracle Identity Manager 11g to 11.1.2*

| Sl No. | Roles in Oracle Identity Manager 11*g* | Roles Removed and Replaced in Oracle Identity Manager 11.1.2 |
|---|---|---|
| 6 | GENERATE_USERNAME_ROLE | Removed and replaced with SYSTEM ADMINISTRATORS. |
| 7 | IDENTITY USER ADMINISTRATORS | Removed and replaced with USER ADMIN. |
| 8 | USER CONFIGURATION ADMINISTRATORS | Removed and replaced with SYSTEM CONFIGURATORS. |
| 9 | ACCESS POLICY ADMINISTRATORS | Removed and replaced with SYSTEM CONFIGURATORS. |
| 10 | RECONCILIATION ADMINISTRATORS | Removed and replaced with SYSTEM ADMINISTRATORS. |
| 11 | RESOURCE ADMINISTRATORS | Removed and replaced with SYSTEM CONFIGURATORS. |
| 12 | GENERIC CONNECTOR ADMINISTRATORS | Removed and replaced with SYSTEM CONFIGURATORS. |
| 13 | APPROVAL POLICY ADMINISTRATORS | Removed and replaced with SYSTEM CONFIGURATORS. |
| 14 | REQUEST ADMINISTRATORS | Removed and replaced with SYSTEM ADMINISTRATORS. |
| 15 | REQUEST TEMPLATE ADMINISTRATORS | Removed and replaced with SYSTEM CONFIGURATORS. |
| 16 | PLUGIN ADMINISTRATORS | Removed and replaced with SYSTEM CONFIGURATORS. |
| 17 | ATTESTATION CONFIGURATION ADMINISTRATORS | Removed and replaced with SYSTEM CONFIGURATORS. |
| 18 | ATTESTATION EVENT ADMINISTRATORS | Removed and replaced with SYSTEM ADMINISTRATORS. |
| 19 | ROLE ADMINISTRATORS | Removed and replaced with ROLE ADMIN. |
| 20 | USER NAME ADMINISTRATOR | Removed and now depends on administration roles. |
| 21 | IDENTITY ORGANIZATION ADMINISTRATORS | Removed and replaced with ORGANIZATION ADMIN. |
| 22 | IT RESOURCE ADMINISTRATORS | Removed and replaced with APPLICATION INSTANCE ADMIN. |
| 23 | REPORT ADMINISTRATORS | No link to reports from Oracle Identity Manager. |
| 24 | SPML_APP_ROLE | There is no change in this enterprise role and a corresponding role with the privileges is seeded in Oracle Entitlements Server. |
| 25 | ALL USERS | This is an enterprise role, not an administrator role. |
| 26 | SYSTEM CONFIGURATORS | All privileges as System Administrator role, except for the ability to manage Users, Roles, Organizations and Provisioning remains unchanged. |
| 27 | SYSTEM ADMINISTRATORS | Remains unchanged. |

### 6.5.19 Verifying the Upgrade

To verify your Oracle Identity Manager upgrade, perform the following steps:

1. Use the following URL in a web browser to verify that Oracle Identity Manager 11.1.2 is running:

   ```
   http://<oim.example.com>:<oim_port>/sysadmin
   ```

   ```
   http://oim.example.com:14000/identity
   ```

   where

   `<oim.example.com>` is the path of the administration console.

   `<oim_port>` is the port number.

2. Use Fusion Middleware Control to verify that Oracle Identity Manager and any other Oracle Identity Management components are running in the Oracle Fusion Middleware environment.

3. Install the Diagnostic Dashboard and run the following tests:

   - Oracle Database Connectivity Check
   - Account Lock Status
   - Data Encryption Key Verification
   - JMS Messaging Verification
   - SOA-Oracle Identity Manager Configuration Check
   - SPML Web Service
   - Test OWSM setup
   - Test SPML to Oracle Identity Manager request invocation
   - SPML attributes to Oracle Identity Manager attributes
   - Username Test

## 6.6 Troubleshooting

For troubleshooting information, see Table 6–18:

*Table 6–18 Oracle Identity Manager Troubleshooting - Problems and Solutions*

| Problem | Solution |
|---|---|
| Patch Set Assistant fails. | Check logs located at:<br>On UNIX:<br>`<MW_HOME>/oracle_common/upgrade/logs/psa<time_stamp>.log`<br>On Windows:<br>`<MW_HOME>\oracle_common\upgrade\logs\psa<time_stamp>.log`<br>Fix the problem, and run Patch Set Assistant again. |

*Table 6–18 (Cont.) Oracle Identity Manager Troubleshooting - Problems and Solutions*

| Problem | Solution |
|---|---|
| Middle Tier upgrade fails | Check logs located at:<br>On UNIX:<br>■ `<OIM_ORACLE_HOME>/server/upgrade/logs/MT/OIMUpgrade<time_stamp>.log`<br>■ `<OIM_ORACLE_HOME>/server/upgrade/logs/MT/ant_JRF.log`<br>■ `<OIM_ORACLE_HOME>/server/upgrade./logs/MT/ant_PatchClasspath.log`<br>On Windows:<br>■ `<OIM_ORACLE_HOME>\server\upgrade\logs\MT\OIMUpgrade<time_stamp>.log`<br>■ `<OIM_ORACLE_HOME>\server\upgrade\logs\MT\ant_JRF.log`<br>■ `<OIM_ORACLE_HOME>\server\upgrade.\logs\MT\ant_PatchClasspath.log` |
| All feature not upgrade in Middle Tier upgrade. | Check the Upgrade Report located at:<br>On UNIX:<br>`<OIM_ORACLE_HOME>/upgrade/logs/MT/oimUpgradeReportDir/index.html`<br>On Windows:<br>`<OIM_ORACLE_HOME>\upgrade\logs\MT\oimUpgradeReportDir\index.html` |
| Oracle Identity Manager upgrade control points. | Set the property value to `true` or `false` in the property file located at:<br>On UNIX:<br>`<OIM_ORACLE_HOME>/server/bin/oimupgrade.properties`<br>On Windows:<br>`<OIM_ORACLE_HOME>\server\bin\oimupgrade.properties`<br>For more information, see Section 6.6.1, "Oracle Identity Manager Upgrade Control Points". |
| MDS patching issues. | Check the MDS Patching Report located at:<br>On UNIX:<br>`<OIM_ORACLE_HOME>/server/logs/MDS_REPORT_DIRECTORY/MDSReport.html`<br>On Windows:<br>`<OIM_ORACLE_HOME>\server\logs\MDS_REPORT_DIRECTORY\MDSReport.html` |

*Table 6–18 (Cont.) Oracle Identity Manager Troubleshooting - Problems and Solutions*

| Problem | Solution |
|---|---|
| Some MDS documents not merged correctly. | Merge manually from the following locations:<br>On UNIX:<br>- `<OIM_ORACLE_HOME>/server/logs/sourceDir` (OOTB MDS data location)<br>- `<OIM_ORACLE_HOME>/server/logs/targetDir` (Your MDS data location)<br>On Windows:<br>- `<OIM_ORACLE_HOME>\server\logs\sourceDir` (OOTB MDS data location)<br>- `<OIM_ORACLE_HOME>\server\logs\targetDir` (Your MDS data location) |
| JDBC errors:<br>ORA-01882: timezone region not found | Add an additional environment variable, TZ, which is the time zone name, like GMT for example. The environment variable has to be set with older database or else you get an error.<br>For more information, see My Oracle Support document ID 1460281.1. |

## 6.6.1 Oracle Identity Manager Upgrade Control Points

Oracle Identity Manager Upgrade has provided some control points in the `oimupgrade.properties`. On UNIX, it is located in the `<OIM_ORACLE_HOME>/server/bin/`directory, on Windows, it is located in the `<OIM_ORACLE_HOME>\server\bin\` directory.

You can selectively disable the feature upgrade by setting the property as `false`.

If any feature fails, you can continue with the upgrade by disabling the failed feature by setting the corresponding feature upgrade property as `false`.

As and when the solution is available for the failed feature, enable the feature for upgrade by setting the property to `true`.

By default, all the properties are set as `true`.

- Set the following property to `false` if you do not want to run Oracle Identity Manager configuration upgrade:

  ```
  oim.ps1.config.patch=true
  ```

- Set the following property to `false` if you do not want to run SOA composite upgrade:

  ```
  oim.ps1.soacomposite.patch=true
  ```

### Domain Extension Properties

- Set the following property to `false` if you do not want to run Patch JNDI provider:

  ```
  oim.domainextension.jndiprovider.patch=true
  ```

- Set the following property to `false` if you do not want to run Patch ClassPath:

  ```
  oim.domainextension.classpath.patch=true
  ```

- Set the following property to `false` if you do not want to run Patch OPSS:

  ```
  oim.domainextension.opss.patch=true
  ```

- Set the following property to `false` if you do not want to run Patch ears:

```
oim.domainextension.ear.patch=true
```

- Set the following property to `false` if you do not want to run Patch JRF:

  ```
  oim.domainextension.jrf.patch=true
  ```

# 7 Upgrading Oracle Entitlements Server 11*g* Release 1 (11.1.1.5.0) Environments

This chapter describes how to upgrade your existing Oracle Entitlements Server 11*g* Release 1 (11.1.1.5.0) environment to Oracle Entitlements Server 11*g* Release 2 (11.1.2).

This chapter contains the following sections:

- Upgrading Oracle Entitlements Server Administration Server
- Upgrading Oracle Entitlements Server Client Server

Read the Oracle Fusion Middleware System Requirements and Specifications document to ensure that your environment meets the minimum requirements for the products you are installing or upgrading.

## 7.1 Upgrading Oracle Entitlements Server Administration Server

This section contains the following topics:

- Upgrade Roadmap for Oracle Entitlements Server Administration Server
- Shutting Down Administration Server and Managed Servers
- Backing Up Oracle Entitlements Server 11g Release 1 (11.1.1.5.0)
- Optional: Upgrading Oracle WebLogic Server
- Upgrading Oracle Entitlements Server Administration Server 11g Release 2 (11.1.2)
- Creating Oracle Platform Security Service Schema
- Creating New Oracle Entitlements Server Domain
- Exporting Encryption Key
- Re-Associating Policy Stores
- Upgrading Oracle Platform Security Services
- Starting the Administration Server and Oracle Entitlements Server Managed Servers
- Redeploying APM
- Verifying the Upgrade

### 7.1.1 Upgrade Roadmap for Oracle Entitlements Server Administration Server

**Note:** If you do not follow the exact sequence provided in this task table, your Oracle Entitlements Server Administration Server upgrade may not be successful.

Table 7–1 lists the steps to upgrade Oracle Entitlements Server Administration Server upgrade.

*Table 7–1 Upgrade Flow*

| Task No. | Task | For More Information |
|---|---|---|
| 1 | Shut down all servers. This includes both Administration Server and Managed Servers. | See, Shutting Down Administration Server and Managed Servers |
| 2 | Back up your environment. | See, Backing Up Oracle Entitlements Server 11g Release 1 (11.1.1.5.0) |
| 3 | Optional - Upgrade Oracle WebLogic Server 10.3.5 to Oracle WebLogic Server 10.3.6. | See, Optional: Upgrading Oracle WebLogic Server |
| 4 | Upgrade 11.1.1.5.0 Oracle Home to 11.1.2. | See, Upgrading Oracle Entitlements Server Administration Server 11g Release 2 (11.1.2) |
| 5 | Create new Oracle Platform Security Services schema. | See, Creating Oracle Platform Security Service Schema |
| 6 | Create new Oracle Entitlements Server domain. | See, Creating New Oracle Entitlements Server Domain |
| 7 | Using the `exportEncryptionKey()`, extract the encryption key. | See, Exporting Encryption Key |
| 8 | Run the `configuresecuritystore.py` script to re-associate policy stores. | See, Re-Associating Policy Stores |
| 9 | Upgrade Oracle Platform Security Services. | See, Upgrading Oracle Platform Security Services |
| 10 | Start the Administration Server and Oracle Entitlements Server Managed servers. | See, Starting the Administration Server and Oracle Entitlements Server Managed Servers |
| 11 | Redeploy APM. | See, Redeploying APM |
| 12 | Verify the Oracle Entitlements Server upgrade. | See, Verifying the Upgrade |

### 7.1.2 Shutting Down Administration Server and Managed Servers

The upgrade process involves changes to the binaries and to the schema. Therefore, before you begin the upgrade process, you must shut down the Administration Server and Managed Servers.

To shut down the Servers, do the following:

#### Stopping the Administration Server

To stop the Administration Server, do the following:

**On UNIX**:

Run the following command:

```
cd <MW_HOME>/user_projects/domains/<domain_name>/bin
```

```
./stopWebLogic.sh
```

**On Windows**:

Run the following command:

```
cd <MW_HOME>\user_projects\domains\<domain_name>\bin
```

```
stopWebLogic.cmd
```

### Stopping the Managed Servers

To stop the Managed Servers, do the following:

**On UNIX**:

1. Move from your present working directory to the `<MW_HOME>/user_projects/domains/<domain_name>/bin` directory by running the following command on the command line:

   ```
   cd <MW_HOME>/user_projects/domains/<domain_name>/bin
   ```

2. Run the following command to stop the servers:

   ```
   ./stopManagedWebLogic.sh <server_name> <admin_url> <user_name>
   <password>
   ```

   where

   `<server_name>` is the name of the Managed Server.

   `<admin_url>` is URL of the administration console. Specify it in the format `http://<host>:<port>/console`. Specify only if the WebLogic Administration Server is on a different computer.

   `<user_name>` is the username of the WebLogic Administration Server.

   `<password>` is the password of the WebLogic Administration Server.

**On Windows**:

1. Move from your present working directory to the `<MW_HOME>\user_projects\domains\<domain_name>\bin` by running the following command on the command line:

   ```
   cd <MW_HOME>\user_projects\domains\<domain_name>\bin
   ```

2. Run the following command to stop the Managed Servers:

   ```
   stopManagedWebLogic.cmd <server_name> <admin_url> <username> <password>
   ```

   where

   `<server_name>` is the name of the Managed Server.

   `<admin_url>` is URL of the administration console. Specify it in the format `http://<host>:<port>/console`. Specify only if the WebLogic Administration Server is on a different computer.

   `<username>` is the username of the WebLogic Administration Server.

   `<password>` is the password of the WebLogic Administration Server.

For more information, see "Stopping the Stack" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

## 7.1.3 Backing Up Oracle Entitlements Server 11*g* Release 1 (11.1.1.5.0)

You must back up your Oracle Entitlements Server 11.1.1.5.0 environment before you upgrade to Oracle Entitlements Server 11.1.2.

After stopping the servers, back up the following:

- *MW_HOME* directory, including the Oracle Home directories inside Middleware Home
- Domain Home directory
- Oracle Entitlements Server schemas

## 7.1.4 Optional: Upgrading Oracle WebLogic Server

**Note:** Upgrading Oracle WebLogic Server is not mandatory. However, Oracle recommends that you upgrade Oracle WebLogic Server to 10.3.6.

You can upgrade WebLogic Server 10.3.5 to Oracle WebLogic Server 10.3.6 by using the WebLogic 10.3.6 Upgrade Installer. Complete the following steps:

1. Download the WebLogic 10.3.6 Upgrade Installer from Oracle Technology Network.

   For more information, see "Downloading the Installer From Oracle Technology Network" in the *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*.

2. Run the Upgrade Installer in graphical mode to upgrade your WebLogic Server.

   For more information, see "Running the Upgrade Installer in Graphical Mode" in the *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*.

## 7.1.5 Upgrading Oracle Entitlements Server Administration Server 11*g* Release 2 (11.1.2)

To upgrade Oracle Entitlements Server Administration Server, you must use the Oracle Identity and Access Management 11.1.2 Installer. During the procedure, point the Middleware Home to your existing 11.1.1.5.0 Middleware Home. Your Oracle Home is upgraded from 11.1.1.5.0 to 11.1.2.

This section contains the following topics:

- Obtaining the Software
- Starting the Oracle Identity and Access Management Installer
- Installing Oracle Identity and Access Management 11g Release 2 (11.1.2)

### 7.1.5.1 Obtaining the Software

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

### 7.1.5.2 Starting the Oracle Identity and Access Management Installer

This topic explains how to start the Oracle Identity and Access Management 11.1.2 Installer.

**Notes:**

- If you are installing 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 doing the following:

**On UNIX**:

1. Move from your present working directory to the directory where you have extracted the contents of the Installer to.
2. Move to the following location:

   ```
   cd Disk1
   ```

3. Run the following command:

   ```
   ./runInstaller -jreLoc <complete path to the JRE directory>
   ```

   For example:

   ```
   ./runInstaller -jreLoc <MW_HOME>/jdk160_29/jre
   ```

**On Windows**:

1. Move from your present working directory to the directory where you have extracted the contents of the Installer to.
2. Move to the following location:

   ```
   cd Disk1
   ```

3. Run the following command:

   ```
   setup.exe -jreLoc <complete path to the JRE directory>
   ```

   For example:

   ```
   setup.exe -jreLoc <MW_HOME>\jdk160_29\jre
   ```

**Note:** 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 is not created in your Middleware Home. You must enter the absolute path to the JRE folder from where your JDK is located.

#### 7.1.5.3 Installing Oracle Identity and Access Management 11*g* Release 2 (11.1.2)

Use the Oracle Identity and Access Management 11.1.2 Installer to upgrade Oracle Entitlements Server 11.1.1.5.0 to Oracle Entitlements Server 11.1.2:

1. After you start the Installer, the **Welcome** screen appears.

2. Click **Next** on the **Welcome** screen. The **Install Software Updates** screen appears. Select whether or not you want to search for updates. Click **Next**.
3. The **Prerequisite Checks** screen appears. If all prerequisite checks pass inspection, click **Next**. The Specify **Installation Location** screen appears.
4. On the **Specify Installation Location** screen, point the Middleware Home to your existing 11.1.1.5.0 Middleware Home installed on your system.
5. In the **Oracle Home Directory** field, specify the path of the existing Oracle Identity and Access Management Home. This directory is also referred to as `<IAM_HOME>` in this book.

   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 you want to proceed with 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**. T**he 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 **Help** on the installation wizard screens.

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

   This installation process copies the 11.1.2 Oracle Identity and Access Management software to your system.

For more information, see "Installing and Configuring Oracle Identity and Access Management (11.1.2)" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

## 7.1.6 Creating Oracle Platform Security Service Schema

> **Note:** You must preform the following task only if your policy store is database.

Oracle Entitlements Server 11.1.1.5.0 schema is bound with APM. From Oracle Entitlements Server 11.1.2 release onwards, Oracle Entitlements Server security store relies on Oracle Platform Security Services for database. In order to access the Oracle Platform Security Services database, you need to create OPSS schema.

Complete the following steps to create Oracle Platform Security Store (OPSS) schema:

1. Run Repository Creation utility (RCU) 11.1.2 to create the schema.

   For more information, see "Creating Schemas" in the *Oracle Fusion Middleware Repository Creation Utility User's Guide*.

**Note:** In the **Select Components** screen, expand **AS Common Schemas** and select **Oracle Platform Security Services**. **Metadata Services** is selected automatically. Deselect it and ignore the following message:

```
Following components require Metadata Services schema:
Oracle Platform Security Services.
```

2. Log in to the database as `SYS`.
3. Go to the following path:

   **On UNIX:**

   `<IAM_HOME>/oes/upgrade/sql`

   **ON Windows:**

   `<IAM_HOME>\oes\upgrade\sql`
4. Run the following sql script:

   `R2_Upgrade.sql`

   This sql script copies the user data from Oracle Entitlements Server 11.1.1.5.0 to Oracle Platform Security Services.

**Note:** In order to execute the `R2_Upgrade.sql` command, you need to install a database client or execute the script in another computer that has a database client installed on it.

### 7.1.7 Creating New Oracle Entitlements Server Domain

Oracle Entitlements Server 11.1.2 Administration applications requires a JRF domain. But Oracle Entitlements Server 11.1.1.5.0 does not support JRF. Therefore, in order to deploy Oracle Entitlements Server 11.1.2 applications, you must create a new Oracle Entitlements Server domain.

For more information, see "Configuring Oracle Entitlements Server in a New WebLogic Domain" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

### 7.1.8 Exporting Encryption Key

Credential data are encrypted and stored in the database. The encryption key is domain specific. Since you are moving to Oracle Entitlements Server 11.1.2 domain from Oracle Entitlements Server 11.1.1.5.0 domain, you must export the key to a keyfile and then import the key to the Oracle Entitlements Server 11.1.2 domain.

You must run the `exportEncryptionKey()`command to extract the encryption key from Oracle Entitlements Server 11.1.1.5.0 domain's bootstrap wallet.

Run the following command:

**On UNIX:**

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

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

2. Run the following command to launch the WebLogic Scripting Tool (WLST):

   ```
   ./wlst.sh
   ```

3. At the WLST prompt, run the following command:

   ```
   exportEncryptionKey(jpsConfigFile="<domaindir>/config/fmwconfig/jps-con
   fig.xml",keyFilePath="/tmp/key",keyFilePassword="<password>")
   ```

   where

   `<domaindir>` is the complete path of the Oracle Entitlements Server 11.1.1.5.0 domain location.

   `<password>` is the key file password.

**On Windows:**

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

   ```
   cd <MW_HOME>\orcle_common\common\bin
   ```

2. Run the following command to launch the WebLogic Scripting Tool (WLST):

   ```
   wlst.cmd
   ```

3. At the WLST prompt, run the following command:

   ```
   exportEncryptionKey(jpsConfigFile="<domaindir>\\config\\fmwconfig\\jps-
   config.xml",keyFilePath="\\tmp\\key",keyFilePassword="<password>")
   ```

   Where

   `<domaindir>` is the complete path of the Oracle Entitlements Server 11.1.1.5.0 domain location.

   `<password>` is the key file password.

### 7.1.9 Re-Associating Policy Stores

You must re-associate policy stores to make the Oracle Entitlements Server 11.1.2 domain uptake the security store which is based on the Oracle Platform Security Services schema. Run the `configuresecuritystore.py` script to re-associate policy stores as follows:

**On UNIX:**

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

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

2. Run the following WLST command:

   ```
   ./wlst.sh <IAM_HOME>/common/tools/configureSecurityStore.py -d
   <domaindir> -m join -j <dwps1 jpsroot> -f <dwps1 farmname> -p <OPSS
   schema password> -s <OPSS data source name> -k <keyFilePath> -w
   <keyFilePassword>
   ```

   For example:

```
./wlst.sh <IAM_HOME>/common/tools/configureSecurityStore.py -d <MW_
HOME>/user_projects/domains/<oes_domain> -m join -j cn=jpsroot -f <oes_
domain> -p welcome1 -s opss-DBDS -k /tmp/key -w myKeyPwd
```

**On Windows:**

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

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

2. Run the following WLST command:

   ```
   wlst.cmd <IAM_HOME>\common\tools\configureSecurityStore.py -d
   <domaindir> -m join -j <OES 11.1.1.5.0 jpsroot> -f <OES 11.1.1.5.0
   farmname> -p <OPSS schema password> -s <OPSS data source name> -k
   <keyFilePath> -w <keyFilePassword>
   ```

   For example:

   ```
   wlst.cmd <IAM_HOME>\common\tools\configureSecurityStore.py -d <MW_
   HOME>\user_projects\domains\<oes_domain> -m join -j cn=jpsroot -f oes_
   domain -p welcome1 -s opss-DBDS -k \tmp\key -w myKeyPwd
   ```

**Note:** If you are using 11*g* Release 2 Bundle Patch 11.1.2.0.1, note the following while running the `configureSecurityStore.py` command:

- Use the argument `--create_diagnostic_data` while running the `configureSecurityStore.py` command. This creates the diagnostic data if it is not already present in your existing security store.

  **On UNIX:**

  ```
  ./wlst.sh <IAM_HOME>/common/tools/configureSecurityStore.py -d
  <domaindir> -m join --create_diagnostic_data -j <dwps1 jpsroot>
  -f <dwps1 farmname> -p <OPSS schema password> -s <OPSS data
  source name> -k <keyFilePath> -w <keyFilePassword>
  ```

  **On Windows:**

  ```
  wlst.cmd <IAM_HOME>\common\tools\configureSecurityStore.py -d
  <domaindir> -m join --create_diagnostic_data -j <OES 11.1.1.5.0
  jpsroot> -f <OES 11.1.1.5.0 farmname> -p <OPSS schema password>
  -s <OPSS data source name> -k <keyFilePath> -w
  <keyFilePassword>
  ```

- You must use the argument `--create_diagnostic_data` only if you are using `-m join` option in the command.

**Note:** For help on the command, run the following:

On UNIX:

```
./wlst.sh <IAM_HOME>/common/tools/configureSecurityStore.py
-d <domaindir> -help
```

On Windows:

```
wlst.cmd <IAM_HOME>\common\tools\configureSecurityStore.py
-d <domaindir> -help
```

Table 7–2 describes the parameters you need to specify on the command line.

*Table 7–2 Parameters for Reassociating Policy Stores*

| Parameter | Description |
|---|---|
| MW_HOME | Specify the path to the Oracle Identity and Access Manager's Middleware Home. The following example shows the complete path:<br>On UNIX, it is located in the /oracle/Middleware directory.<br>On Windows, it is located in the \oracle\Middleware directory. |
| IAM_HOME | Specify the path to the Oracle Identity and Access Manager Home. The following example shows the complete path:<br>On UNIX, it is located in the /oracle/Middleware/Oracle_IDM1 directory.<br>On Windows, it is located in the \oracle\Middleware\Oracle_IDM1 directory. |
| domaindir | Specify the path to the Identity and Access Manager's domain location. The following example shows the complete path:<br>On UNIX, it is located in the <MW_HOME>/user_projects/domains/base_domain directory.<br>On Windows, it is located in the <MW_HOME>\user_projects\domains\base_domain directory. |
| -m | The following are the two options available for the argument -m:<br>▪ create<br>-m create option creates a new security store. This option is applicable for fresh installation.<br>▪ join<br>-m join option uses an existing database security store for the domain. Since this is an upgrade, you must use -m join option while running the configureSecurityStore.py command. |
| OPSS_schema_ password | Specify the password of OPSS schema. |
| -k | Specify the path to the KeyFile. The following example shows the complete location:<br>On UNIX, it is located at /tmp/key<br>On Windows, it is located at \tmp\key |
| -w | Specify the KeyFile password. |

## 7.1.10 Upgrading Oracle Platform Security Services

Upgrading Oracle Platform Security Services (OPSS) is required to upgrade the configuration and policy stores of Oracle Entitlements Server 11.1.1.5.0 to Oracle Entitlements Server 11.1.2. It upgrades the jps-config.xml file and policy stores.

### For Database

To upgrade Oracle Platform Security Services (OPSS), do the following:

### On UNIX:

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

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

2. Run the following command to launch the WebLogic Scripting Tool (WLST):

```
./wlst.sh
```

3. At the WLST prompt, run the following command:

```
upgradeOpss(jpsConfig="existing_jps_config_file", jaznData="system_
jazn_data_file")
```

For example:

```
upgradeOpss(jpsConfig="<MW_HOME>/user_projects/domains/base_
domain/config/fmwconfig/jps-config.xml",jaznData="<MW_HOME>/oracle_
common/modules/oracle.jps_11.1.1/domain_config/system-jazn-data.xml")
```

4. Exit the WLST console using the `exit()`command.

### On Windows:

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

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

2. Run the following command to launch the WebLogic Scripting Tool (WLST):

```
wlst.cmd
```

3. At the WLST prompt, run the following command:

```
upgradeOpss(jpsConfig="existing_jps_config_file", jaznData="system_
jazn_data_file")
```

For example:

```
upgradeOpss(jpsConfig="<MW_HOME>\\user_projects\\domains\\base_
domain\\config\\fmwconfig\\jps-config.xml",jaznData="<MW_HOME>\\oracle_
common\\modules\\oracle.jps_11.1.1\\domain_
config\\system-jazn-data.xml")
```

4. Exit the WLST console using the `exit()` command.

Table 7–3 describes the parameters you specify on the command line:

***Table 7–3 Parameters for Upgrading OPSS***

| Parameter | Description |
|---|---|
| `jpsConfig` | Specify the path to the `jps-config.xml` file in your 11.1.2 installation. The following example shows the complete path:<br>On UNIX, it is located in the `<MW_HOME>/user_projects/domains/base_domain/config/fmwconfig/jps-config.xml` directory.<br>On Windows, it is located in the `<MW_HOME>\user_projects\domains\base_domain\config\fmwconfig\jps-config.xml directory.` |

*Table 7–3 (Cont.) Parameters for Upgrading OPSS*

| Parameter | Description |
|---|---|
| jaznData | Specify the path to the system-jazn-data.xml file in your 11.1.2 installation. The following example shows the complete path:<br>On UNIX, it is located in the `<MW_HOME>/oracle_common/modules/oracle.jps_11.1.1/domain_config/system-jazn-data.xml` directory.<br>On Windows, it is located in the `<MW_HOME>\oracle_common\modules\oracle.jps_11.1.1\domain_config\system-jazn-data.xml` directory. |

### For LDAP

To upgrade Oracle Platform Security Services (OPSS), do the following:

### On UNIX

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

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

2. Run the following command to launch the WebLogic Scripting Tool (WLST):

   ```
   ./wlst.sh
   ```

3. At the WLST prompt, run the following command:

   ```
   upgradeOpss(jpsConfig="existing_jps_config_file", jaznData="system_
   jazn_data_file")
   ```

   **For example:**

   ```
   upgradeOpss(jpsConfig="<MW_HOME>/user_projects/domains/base_
   domain/config/fmwconfig/jps-config.xml",jaznData="<MW_HOME>/user_
   projects/domains/base_domain/config/fmwconfig/system-jazn-data.xml")
   ```

4. Exit the WLST console using the `exit()` command.

### On Windows:

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

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

2. Run the following command:

   ```
   wlst.cmd
   ```

3. Run the following script:

   ```
   upgradeOpss(jpsConfig="existing_jps_config_file", jaznData="system_
   jazn_data_file")
   ```

   **For example:**

   ```
   upgradeOpss(jpsConfig="<MW_HOME>\\user_projects\\domains\\base_
   domain\\config\\fmwconfig\\jps-config.xml",jaznData="<MW_HOME>\\user_
   projects\\domains\\base_
   domain\\config\\fmwconfig\\system-jazn-data.xml")
   ```

4. Exit the WLST console using the `exit()` command.

Table 7–4 describes the parameters you specify on the command line:

*Table 7–4 Parameters for upgrading OPSS*

| Parameter | Description |
|---|---|
| `jpsConfig` | Specify the path to the jps-config.xml file in your 11.1.2 installation. The following example shows the complete path:<br>On UNIX, it is located in the `<MW_HOME>/user_projects/domains/base_domain/config/fmwconfig/jps-config.xml` directory.<br>On Windows, it is located in the `<MW_HOME>\user_projects\domains\base_domain\config\fmwconfig\jps-config.xml` directory. |
| `jaznData` | Specify the path to the jaznData file in your 11.1.2 installation. The following example shows the complete path:<br>On UNIX, it is located in the `<MW_HOME>/user_projects/domains/base_domain/config/fmwconfig/system-jazn-data.xml` directory.<br>On Windows, it is located in the `<MW_HOME>\user_projects\domains\base_domain\config\fmwconfig\system-jazn-data.xml` directory. |

## 7.1.11 Starting the Administration Server and Oracle Entitlements Server Managed Servers

After the upgrade is complete, start the WebLogic Administration Server, the Administration Server for the domain that contains Oracle Entitlements Server, and the Oracle Entitlements Server Managed Server by running the following commands on the command line:

### Starting Administration Server

To start the Administration Server, do the following:

**On UNIX**:

Run the following command:

```
cd <MW_HOME>/user_projects/domains/<domain_name>/bin
```

```
./startWebLogic.sh
```

**On Windows**:

Run the following command:

```
cd <MW_HOME>\user_projects\domains\<domain_name>\bin
```

```
startWebLogic.cmd
```

### Starting Managed Servers

To start the Managed Servers, do the following:

**On UNIX**:

1. Move from your present working directory to the `<MW_HOME>/user_projects/domains/<domain_name>/bin` directory by running the following command on the command line:

   ```
   cd <MW_HOME>/user_projects/domains/<domain_name>/bin
   ```

2. Run the following command to start the Managed Servers:

   ```
   ./startManagedWebLogic.sh <managed_server_name> <admin_url> <user_name>
   <password>
   ```

   where

   `<managed_server_name>` is the name of the Managed Server

   `<admin_url>` is URL of the administration console. Specify it in the format `http://<host>:<port>/console`. Specify only if the WebLogic Administration Server is on a different computer.

   `<user_name>` is the username of the WebLogic Administration Server.

   `<password>` is the password of the WebLogic Administration Server.

**On Windows**:

1. Move from your present working directory to the `<MW_HOME>\user_projects\domains\<domain_name>\bin` directory by running the following command on the command line:

   ```
   cd <MW_HOME>\user_projects\domains\<domain_name>\bin
   ```

2. Run the following command to start the Managed Servers:

   ```
   startManagedWebLogic.cmd <managed_server_name> <admin_url> <user_name>
   <password>
   ```

   where

   `<managed_server_name>` is the name of the Managed Server.

   `<admin_url>` is URL of the administration console. Specify it in the format `http://<host>:<port>/console`. Specify only if the WebLogic Administration Server is on a different computer.

   `<user_name>` is the username of the WebLogic Administration Server.

   `<password>` is the password of the WebLogic Administration Server.

For more information, see "Starting the Stack" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

## 7.1.12 Redeploying APM

To get the latest APM policies into the policy store, you must redeploy the APM applications.

Complete the following steps to redeploy APM:

**On UNIX:**

1. Move from your present working directory to the `<MW_HOME>/wlserver_10.3/common/bin` directory by running the following command on the command line:

   ```
   cd <MW_HOME>/wlserver_10.3/common/bin
   ```

2. Run the following command to launch the WebLogic Scripting Tool (WLST):

   ```
   ./wlst.sh
   ```

3. Connect to the Administration Server using the following command:

   ```
   connect('weblogic-username','weblogic-password','weblogic-url')
   ```

4. At the WLST prompt, run the following command:

   ```
   redeploy(appName='oracle.security.apm')
   ```

5. Exit the WLST console using the `exit()` command.

**On Windows:**

1. Move from your present working directory to the `<MW_HOME>\wlserver_10.3\common\bin` by running the following command on the command line:

   ```
   cd <MW_HOME>\wlserver_10.3\common\bin
   ```

2. Run the following command to launch the WebLogic Scripting Tool (WLST):

   ```
   wlst.cmd
   ```

3. Connect to the Administration Server using the following command:

   ```
   connect('weblogic-username','weblogic-password','weblogic-url')
   ```

4. At the WLST prompt, run the following command:

   ```
   <domaindir>\serverConfig\redeploy(appName='oracle.security.apm')
   ```

   where

   `<domaindir>` is the complete path to the Oracle Entitlements Server 11.1.2 domain.

   **For example:**

   ```
   <MW_HOME>\user_projects\domains\<oes_domain>\serverConfig\
   redeploy(appName='oracle.security.apm')
   ```

5. Exit the WLST console using the `exit()` command.

### 7.1.13 Verifying the Upgrade

To verify the Oracle Entitlements Server upgrade, do the following:

- Log in to LDAP or database and verify the schema version in the PolicyStore. The version number should be 11.1.2.
- The application MAPI works with both old and new functionalities.

  Create a new policy to see if CRUD operations on the policy store artifacts, using their entity managers, are working.

  For more information, see "Creating Fine Grained Elements for a Simple Policy" in the *Oracle Fusion Middleware Developer's Guide for Oracle Entitlements Server*.
- The Application Runtime Authorization continues working.

  To verify, create an authorization, as mentioned in "Using the PEP API" in the *Oracle Fusion Middleware Developer's Guide for Oracle Entitlements Server*, and see if it works correctly.

## 7.2 Upgrading Oracle Entitlements Server Client Server

This section contains the following topics:

- Stopping all Security Module Instances
- Upgrading Oracle Entitlements Server Client 11g Release 2 (11.1.2)
- Changing Username and Password for the New Schemas
- Starting the Security Modules

- Verifying the Upgrade

### 7.2.1 Upgrade Roadmap for Oracle Entitlements Server Administration Server

**Note:** If you do not follow the exact sequence provided in this task table, your Oracle Entitlements Server Client Server upgrade may not be successful.

Table 7–5 lists the steps for upgrading Oracle Entitlements Server Client Server upgrade.

*Table 7–5 Upgrade Flow*

| Sl. No. | Task | For More Information |
|---|---|---|
| 1 | Shut down all security modules. This includes shutting down the Administration Server and Managed Servers too. | See, Stopping all Security Module Instances |
| 2 | Upgrade 11.1.1.5.0 Oracle Home to 11.1.2. | See, Upgrading Oracle Entitlements Server Client 11g Release 2 (11.1.2) |
| 3 | Change the username and password. | See, Changing Username and Password for the New Schemas |
| 4 | Start the security modules. | See, Starting the Security Modules |
| 5 | Verify the Oracle Entitlements Server Client Server upgrade. | See, Verifying the Upgrade |

### 7.2.2 Stopping all Security Module Instances

Bring down all security module instances, Administration Server, and Managed Servers.

The security module instances shuts down when the Administration Server and Managed Servers are shut down.

To stop the servers, see Section 7.1.2, "Shutting Down Administration Server and Managed Servers".

### 7.2.3 Upgrading Oracle Entitlements Server Client 11*g* Release 2 (11.1.2)

To upgrade Oracle Entitlements Server Client Server, you must use the 11.1.2 installer. During the procedure, point the Middleware Home to your existing 11.1.1.5.0 Oracle Entitlements Server Middleware Home. This upgrades your Middleware Home and Oracle Home from 11.1.1.5.0 to 11.1.2.

This section contains the following topics:

- Prerequisites
- Obtaining the Software
- Installing Oracle Entitlements Server Client Server 11g Release 2 (11.1.2)
- Verifying the Installation

#### 7.2.3.1 Prerequisites

You must install and configure Oracle Entitlements Server Administration Server, as described in Section 7.1.5, "Upgrading Oracle Entitlements Server Administration Server 11g Release 2 (11.1.2)".

#### 7.2.3.2 Obtaining the Software

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

#### 7.2.3.3 Installing Oracle Entitlements Server Client Server 11*g* Release 2 (11.1.2)

For more information on installing Oracle Entitlements Server Client Server 11.1.2, see "Installing Oracle Entitlements Server Client" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

#### 7.2.3.4 Verifying the Installation

To verify that your Oracle Entitlements Server Client install was successful, go to your Oracle Home directory which you specified during installation and verify that the Oracle Entitlements Server Client installation files are created.

### 7.2.4 Changing Username and Password for the New Schemas

If Oracle Entitlements Server client is running in a controlled-pull mode or in an uncontrolled mode, the `jps-config.xml` of the Security Module instance must be changed to reflect the schema changes done during the Administration Server upgrade.

Before running the `oessmconfig.sh` command, you need to modify `jps-config.xml` of the controlled-pull or uncontrolled security module.

**Controlled-Pull Security Module**

For controlled-pull security module, add the following to the `pdp.service` instance:

```
<property name="oracle.security.jps.runtime.pd.client.SMinstanceType"
value="<sm_type>"/>
```

Replace `"<sm_type>"` with the actual type.

For example:

```
"java"
```

**Uncontrolled Security Module**

For uncontrolled security module, add the following to the `pdp.service` instance:

```
<property
name="oracle.security.jps.runtime.pd.client.policyDistributionMode"
value="non-controlled"/>
```

```
<property name="oracle.security.jps.runtime.pd.client.sm_name" value="<sm_
name>"/>
```

```
<property name="oracle.security.jps.runtime.pd.client.SMinstanceType"
value="<sm_type>"/>
```

Replace `"<sm_name>" "<sm_type>"` with the actual values.

Do the following to change the username and password of the new schemas:

1. Go to the following path:

   On UNIX, `<CLIENT_HOME>/oesclient/oessm/enroll/bin`

   On Windows, `<CLIENT_HOME>\oesclient\oessm\enroll\bin`

2. Run the following command:

   On UNIX:

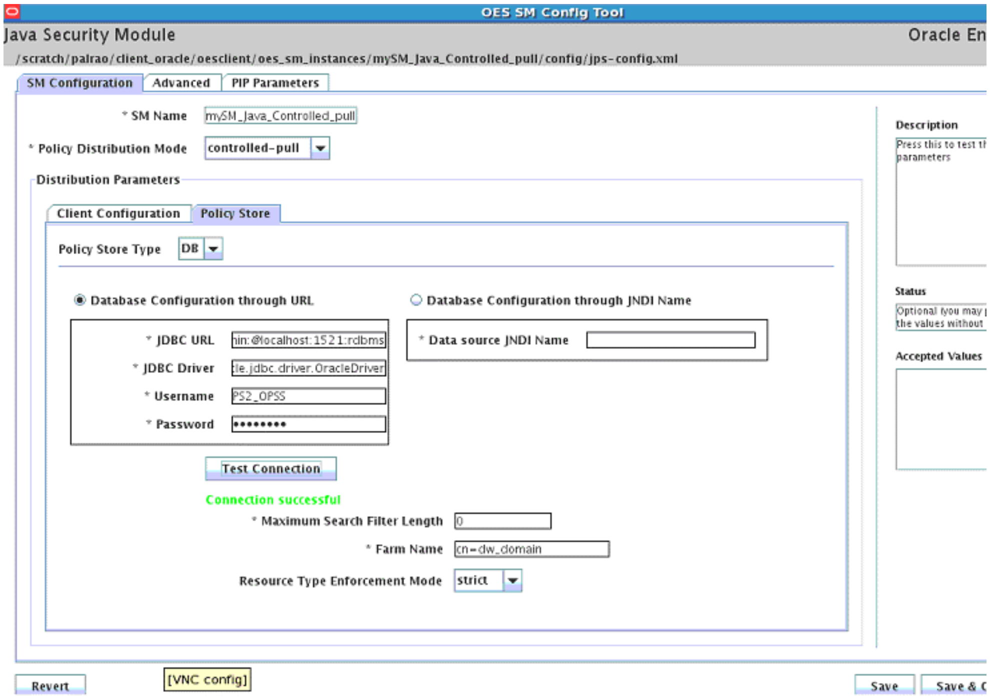
   ```
   ./oessmconfig.sh -jpsconfig <path to the jps-config.xml>
   ```

   On Windows:

   ```
   oessmconfig.cmd -jpsconfig <path to the jps-config.xml>
   ```

3. A Graphic User Interface displays. See Figure 7–1.
4. Click **SM Configuration**.
5. Click the **Policy Store** sub-tab.
6. Enter the new schema user name and password.
7. Click **Test Connection**
8. When you get the successful security module test message, click **Save & Close**.

***Figure 7–1 Java Security Module***



OES SM Config Tool

Java Security Module

/scratch/palrao/client_oracle/oesclient/oes_sm_instances/mySM_Java_Controlled_pull/config/jps-config.xml

* SM Name: mySM_Java_Controlled_pull

* Policy Distribution Mode: controlled-pull

Distribution Parameters

Policy Store Type: DB

● Database Configuration through URL

* JDBC URL: hin:@localhost:1521:rdbms

* JDBC Driver: :le.jdbc.driver.OracleDriver

* Username: PS2_OPSS

* Password: ••••••••

○ Database Configuration through JNDI Name

* Data source JNDI Name:

Connection successful

* Maximum Search Filter Length: 0

* Farm Name: cn=dw_domain

Resource Type Enforcement Mode: strict

Description: Press this to test th parameters

Status: Optional (you may p the values without

Accepted Values

## 7.2.5 Starting the Security Modules

You must start the security modules by starting the Administration Server and Managed Servers.

To start the servers, see Section 7.1.11, "Starting the Administration Server and Oracle Entitlements Server Managed Servers".

### 7.2.6 Verifying the Upgrade

To verify, create an authorization, as mentioned in "Using the PEP API" in the *Oracle Fusion Middleware Developer's Guide for Oracle Entitlements Server*, and see if it works correctly.

The Application Runtime Authorization continues working.

# 8

# Upgrading Oracle Identity Navigator 11*g* Release 1 (11.1.1.5.0) Environments

This chapter describes how to upgrade your existing Oracle Identity Navigator 11*g* Release 1 (11.1.1.5.0) to Oracle Identity Navigator 11*g* Release 2 (11.1.2).

This chapter includes the following sections:

- Upgrade Roadmap for Oracle Identity Navigator
- Exporting Oracle Identity Navigator 11.1.1.5.0 Metadata
- Shutting Down Administration Server and Managed Servers
- Optional: Upgrading Oracle WebLogic Server
- Upgrading Oracle Identity Navigator 11g Release 2 (11.1.2)
- Creating Oracle Platform Security Services Schema
- Extending Oracle Identity Navigator 11.1.1.5.0 Component Domains with Oracle Platform Security Services Template
- Upgrading Oracle Platform Security Services
- Configuring Oracle Platform Security Services Security Store
- Starting the Administration Server
- Verifying the Deployment Summary
- Upgrading Oracle Identity Navigator Application
- Importing the Oracle Identity Navigator 11.1.2 Metadata
- Verifying the Upgrade

Read the Oracle Fusion Middleware System Requirements and Specifications document to ensure that your environment meets the minimum requirements for the products you are installing or upgrading.

## 8.1 Upgrade Roadmap for Oracle Identity Navigator

> **Note:** If you do not follow the exact sequence provided in this task table, your Oracle Identity Navigator upgrade may not be successful.

Table 8–1 lists the steps to upgrade Oracle Identity Navigator.

*Table 8–1 Upgrade Flow*

| So. No. | Task | For More Information |
|---|---|---|
| 1 | Export Oracle Identity Navigator data. | See, Exporting Oracle Identity Navigator 11.1.1.5.0 Metadata |
| 2 | Shut down all servers. This includes both Administration Server and Managed Servers. | See, Shutting Down Administration Server and Managed Servers |
| 3 | Optional - Upgrade Oracle WebLogic Server 10.3.5 to Oracle WebLogic Server 10.3.6. | See, Optional: Upgrading Oracle WebLogic Server |
| 4 | Upgrade 11.1.1.5.0 Oracle Home to 11.1.2. | See, Upgrading Oracle Identity Navigator 11g Release 2 (11.1.2) |
| 5 | Run Oracle Fusion Middleware Repository Creation Utility (RCU) to create and load OPSS schema for Oracle Identity and Access Management products. | See, Creating Oracle Platform Security Services Schema |
| 6 | Extend your Oracle Identity Navigator 11.1.1.5.0 domain with the OPSS template. | See, Extending Oracle Identity Navigator 11.1.1.5.0 Component Domains with Oracle Platform Security Services Template |
| 7 | Upgrade Oracle Platform Security Services. | See, Upgrading Oracle Platform Security Services |
| 8 | Run the `configuresecuritystore.py` script to configure policy stores. | See, Configuring Oracle Platform Security Services Security Store |
| 9 | Start the Administration Server. | See, Starting the Administration Server |
| 10 | Verify the deployments summary. | See, Verifying the Deployment Summary |
| 11 | Upgrade Oracle Identity Navigator. | See, Upgrading Oracle Identity Navigator Application |
| 12 | Import data. | See, Importing the Oracle Identity Navigator 11.1.2 Metadata |
| 13 | Verify the Oracle Identity Navigator upgrade. | See, Verifying the Upgrade |

## 8.2 Exporting Oracle Identity Navigator 11.1.1.5.0 Metadata

OINAV uses MDS as its metadata store. During upgrade, when you update the application, the metadata gets overwritten. Therefore, you need to export it and keep it in a temporary location so that it can be used to import original metadata after upgrade.

On the computer where Oracle Identity Navigator 11.1.1.5.0 is installed, export the Oracle Identity Navigator metadata to an export directory using WLST as follows:

**On UNIX:**

1. Move from your present working directory to the `<IAM_HOME>/common/bin` directory by running the following command on the command line:

   ```
   cd <IAM_HOME>/common/bin
   ```

2. Run the following command to launch the WebLogic Scripting Tool (WLST):

   ```
   ./wlst.sh
   ```

3. Connect to the Administration Server using the following command:

   ```
   connect('weblogic-username','weblogic-password','weblogic-url')
   ```

4. At the WLST prompt, run the following WLST (online) command:

   ```
   exportMetadata(application='oinav',server='AdminServer',toLocation='exp
   ort_directory')
   ```

   where

   `export_directory` is the directory where you want to export Oracle Identity Navigator metadata to.

**On Windows:**

1. Move from your present working directory to the `<IAM_HOME>\common\bin` directory by running the following command on the command line:

   ```
   cd <IAM_HOME>\common\bin
   ```

2. Run the following command to launch the WebLogic Scripting Tool (WLST):

   ```
   wlst.cmd
   ```

3. Connect to the Administration Server using the following command:

   ```
   connect('weblogic-username','weblogic-password','weblogic-url')
   ```

4. At the WLST prompt, run the following WLST (online) command:

   ```
   exportMetadata(application='oinav',server='AdminServer',toLocation='exp
   ort_directory')
   ```

   where

   `export_directory` is the directory where you want to export Oracle Identity Navigator metadata to.

## 8.3 Shutting Down Administration Server and Managed Servers

The upgrade process involves changes to the binaries and to the schema. So, before you begin the upgrade process, you must shut down the Administration Server and Managed Servers.

To shut down the Servers, do the following:

### Stopping the Administration Server

To stop the Administration Server, do the following:

**On UNIX**:

Run the following command:

```
cd <MW_HOME>/user_projects/domains/<domain_name>/bin
```

./stopWebLogic.sh

**On Windows**:

Run the following command:

```
cd <MW_HOME>\user_projects\domains\<domain_name>\bin
```

stopWebLogic.cmd

### Stopping Managed Servers

To stop the Managed Servers, do the following:

**On UNIX**:

1. Move from your present working directory to the `<MW_HOME>/user_projects/domains/<domain_name>/bin` directory by running the following command on the command line:

   ```
   cd <MW_HOME>/user_projects/domains/<domain_name>/bin
   ```

2. Run the following command to stop the Managed Servers:

   ```
   ./stopManagedWebLogic.sh <server_name> <admin_url> <user_name>
   <password>
   ```

   where

   `<server_name>` is the name of the Managed Server.

   `<admin_url>` is URL of the WebLogic administration console. Specify it in the format `http://<host>:<port>/console`. Specify only if the WebLogic Administration Server is on a different computer.

   `<user_name>` is the username of the WebLogic Administration Server.

   `<password>` is the password of the WebLogic Administration Server.

**On Windows**:

1. Move from your present working directory to the `<MW_HOME>\user_projects\domains\<domain_name>\bin` directory by running the following command on the command line:

   ```
   cd <MW_HOME>\user_projects\domains\<domain_name>\bin
   ```

2. Run the following command to stop the Managed Servers:

   ```
   stopManagedWebLogic.cmd <server_name> <admin_url> <username> <password>
   ```

   where

   `<server_name>` is the name of the Managed Server.

   `<admin_url>` is URL of the Weblogic administration console. Specify it in the format `http://<host>:<port>/console`. Specify only if the WebLogic Administration Server is on a different computer.

   `<username>` is the username of the WebLogic Administration Server.

   `<password>` is the password of the WebLogic Administration Server.

## 8.4 Optional: Upgrading Oracle WebLogic Server

> **Note:** Upgrading Oracle WebLogic Server is not mandatory. However, Oracle recommends that you upgrade Oracle WebLogic Server to 10.3.6.

You can upgrade WebLogic Server 10.3.5 to Oracle WebLogic Server 10.3.6 by using the WebLogic 10.3.6 Upgrade Installer. Complete the following steps:

1. Download the WebLogic 10.3.6 Upgrade Installer from Oracle Technology Network.

For more information, see "Downloading the Installer From Oracle Technology Network" in the *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*.

2. Run the Upgrade Installer in graphical mode to upgrade your WebLogic Server.

   For more information, see "Running the Upgrade Installer in Graphical Mode" in the *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*.

## 8.5 Upgrading Oracle Identity Navigator 11*g* Release 2 (11.1.2)

To upgrade Oracle Identity Navigator, you must use the Oracle Identity and Access Management 11.1.2 Installer. During the procedure, point the Middleware Home to your existing 11.1.1.5.0 Oracle Identity Navigator Middleware Home. Your Oracle Home is upgraded from 11.1.1.5.0 to 11.1.2.

This section contains the following topics:

- Obtaining the Software
- Starting the Oracle Identity and Access Management Installer
- Installing Oracle Identity and Access Management 11g Release 2 (11.1.2)

### 8.5.1 Obtaining the Software

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

### 8.5.2 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 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 doing the following:

**On UNIX**:

1. Move from your present working directory to the directory where you extracted the contents of the Installer to.
2. Move to the following location:

   ```
   cd Disk1
   ```

3. Run the following command:

   ```
   ./runInstaller -jreLoc <complete path to the JRE directory>
   ```

   For example:

   ```
   ./runInstaller -jreLoc <MW_HOME>/jdk160_29/jre
   ```

**On Windows**:

1. Move from your present working directory to the directory where you extracted the contents of the Installer to.
2. Move to the following location:

   ```
   cd Disk1
   ```

3. Run the following command:

   ```
   setup.exe -jreLoc <complete path to the JRE directory>
   ```

   For example:

   ```
   setup.exe -jreLoc <MW_HOME>\jdk160_29\jre
   ```

> **Note:** 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 is not created in your Middleware Home. You must enter the absolute path to the JRE folder from where your JDK is located.

### 8.5.3 Installing Oracle Identity and Access Management 11*g* Release 2 (11.1.2)

Use Oracle Identity and Access Management 11.1.2 Installer to upgrade Oracle Identity Navigator 11.1.1.5.0 to Oracle Identity Navigator 11.1.2:

1. After you start the Installer, the **Welcome** screen appears.
2. Click **Next** on the **Welcome** screen. The **Install Software Updates** screen appears. Select whether or not you want to search for updates. Click **Next**.
3. The **Prerequisite Checks** screen appears. If all prerequisite checks pass inspection, click **Next**. The **Specify Installation Location** screen appears.
4. On the **Specify Installation Location** screen, point the Middleware Home to your existing 11.1.1.5.0 Middleware Home installed on your system.
5. In the **Oracle Home Directory** field, specify the path of the existing Oracle Identity and Access Management Home. This directory is also referred to as <IAM_HOME> in this book.

   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 you want to proceed with 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 **Help** on the installation wizard screens.

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

   This installation process copies the 11.1.2 Oracle Identity and Access Management software to your system.

For more information, see "Installing and Configuring Oracle Identity and Access Management (11.1.2)" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

## 8.6 Creating Oracle Platform Security Services Schema

You must create Oracle Platform Security Services (OPSS) schema because Oracle Identity Navigator upgrade process involves OPSS schema policy store changes. The keys, roles, permissions, and other artifacts used by the applications must migrate to the policy store.

Run Repository Creation utility (RCU) to create OPSS schema.

For more information, see "Creating Schemas" in the *Oracle Fusion Middleware Repository Creation Utility User's Guide*.

**Note:** In the **Select Components** screen, expand **AS Common Schemas** and select **Oracle Platform Security Services**. The **Metadata Services** schema is selected automatically.

## 8.7 Extending Oracle Identity Navigator 11.1.1.5.0 Component Domains with Oracle Platform Security Services Template

Oracle Identity Navigator 11.1.2 uses the database to store policies. This requires extending the 11.1.1.5.0 Oracle Identity Navigator domain to include the OPSS data source.

To do so, complete the following steps:

1. Run the following command to launch the Oracle Fusion Middleware configuration wizard:

   **On UNIX:**

   ```
   ./config.sh
   ```

   It is located in the `<MW_HOME>/Oracle_IDM1/common/bin` directory.

   **On Windows:**

   ```
   config.cmd
   ```

   It is located in the `<MW_HOME>\Oracle_IDM1\common\bin` directory.

2. On the **Welcome** screen, select the **Extend an existing WebLogic domain** option. Click **Next**.

3. On the **Select a WebLogic Domain Directory** screen, browse to the directory that contains the WebLogic domain in which you configured the components. Click **Next**. The **Select Extension Source** screen is displayed.
4. On the **Select Extension Source** screen, select the **Oracle Platform Security Service - 11.1.1.0 [Oracle_IDM1]** option. After selecting the domain configuration options, click **Next**.
5. The **Configure JDBC Data Sources** screen is displayed. Configure the opssDS data source, as required. After the test succeeds, the **Configure JDBC Component Schema** screen is displayed.
6. On the **Configure JDBC Component Schema** screen, select the **Oracle Platform Security Services** schema.

   You can set values for Schema Owner, Schema Password, Database and Service, Host Name, and Port. Click **Next**.

   The **Test JDBC Component Schema** screen is displayed. After the test succeeds, the **Select Optional Configuration** screen is displayed.
7. On the **Select Optional Configuration** screen, you can configure Managed Servers, Clusters, and Machines and Deployments and Services. Do not select anything as you have already configured in your Oracle Identity Navigator 11.1.1.5.0 environment. Click **Next**.
8. On the **Configuration Summary** screen, review the domain configuration, and click **Extend** to start extending the domain.

Your existing Oracle Identity Navigator domain is extended to support Oracle Platform Security Services (OPSS).

## 8.8 Upgrading Oracle Platform Security Services

To upgrade Oracle Platform Security Services (OPSS) schema, do the following:

**On UNIX:**

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

   ```
   cd <MW_HOME>/oracle_common/common/bin
   ```
2. Run the following command to launch the WebLogic Scripting Tool (WLST):

   ```
   ./wlst.sh
   ```
3. At the WLST prompt, run the following command:

   ```
   upgradeOpss(jpsConfig="existing_jps_config_file", jaznData="system_
   jazn_data_file")
   ```

   For example:

   ```
   upgradeOpss(jpsConfig="<MW_HOME>/user_projects/domains/base_
   domain/config/fmwconfig/jps-config.xml",jaznData="<MW_HOME>/oracle_
   common/modules/oracle.jps_11.1.1/domain_config/system-jazn-data.xml")
   ```
4. Exit the WLST console using the `exit()`command.

**On Windows:**

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

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

2. Run the following command to launch the WebLogic Scripting Tool (WLST):

   ```
   wlst.cmd
   ```

3. At the WLST prompt, run the following command:

   ```
   upgradeOpss(jpsConfig="existing_jps_config_file", jaznData="system_
   jazn_data_file")
   ```

   For example:

   ```
   upgradeOpss(jpsConfig="<MW_HOME>\\user_projects\\domains\\base_
   domain\\config\\fmwconfig\\jps-config.xml",jaznData="<MW_HOME>\\oracle_
   common\\modules\\oracle.jps_11.1.1\\domain_
   config\\system-jazn-data.xml")
   ```

4. Exit the WLST console using the exit() command.

Table 8–2 describes the parameters you need to specify on the command line:

*Table 8–2 Parameters for Upgrading OPSS*

| Parameter | Description |
|---|---|
| jpsConfig | Specify the path to the jps-config.xml file in your 11.1.2 installation. The following example shows the complete path:<br>On UNIX, it is located in the <MW_HOME>/user_projects/domains/base_domain/config/fmwconfig/jps-config.xml directory.<br>On Windows, it is located in the <MW_HOME>\user_projects\domains\base_domain\config\fmwconfig\jps-config.xml directory. |
| jaznData | Specify the path to the system-jazn-data.xml file in your 11.1.2 installation. The following example shows the complete path:<br>On UNIX, it is located in the <MW_HOME>/oracle_common/modules/oracle.jps_11.1.1/domain_config/system-jazn-data.xml directory.<br>On Windows, it is located in the <MW_HOME>\oracle_common\modules\oracle.jps_11.1.1\domain_config\system-jazn-data.xml directory. |

## 8.9 Configuring Oracle Platform Security Services Security Store

You must configure the Database Security Store as it is the only security store type supported by Oracle Identity and Access Management 11g Release 2 (11.1.2).

For more information on configuring Oracle Platform Security Services, see "Configuring Database Security Store for an Oracle Identity and Access Management Domain" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

## 8.10 Starting the Administration Server

After the upgrade is complete, start the WebLogic Administration Server, the Administration Server that contains the Oracle Identity Navigator console, by running the following command on the command line:

**On UNIX**:

```
cd <MW_HOME>/user_projects/domains/<domain_name>/bin
```

```
./startWebLogic.sh
```

**On Windows**:

```
cd <MW_HOME>\user_projects\domains\<domain_name>\bin
```

```
startWebLogic.cmd
```

## 8.11 Verifying the Deployment Summary

To verify the deployment summary, do the following:

1. Log in to the WebLogic Administration console:

   ```
   http://<admin server host>:<admin server port>/console
   ```

2. Under Domain Structure, click **Deployments**. The Summary of Deployments page is displayed.
3. Check the summary details and verify that **oinav (11.1.1.3.0)** is present in the Name table.

## 8.12 Upgrading Oracle Identity Navigator Application

> **Note:** The OINAV version number is 11.1.1.3.0 while the Oracle Identity Navigator version number is 11.1.2.
>
> This is not an error. The discrepancy is caused by a difference between how OINAV and Identity Access Management releases are tracked internally.

Upgrading Oracle Identity Navigator redeploys Oracle Identity Navigator using `oinav.ear` for Oracle Identity Navigator 11.1.2 release. There are two ways of redeploying the `oinav.ear`:

- Upgrading `oinav` using the WebLogic Server Administration Console.
- Upgrading `oinav` using the WebLogic Scripting Tool (WLST).

### Using WebLogic Server Administration Console

Complete the following steps to upgrade Oracle Identity Navigator through the WebLogic Administration console:

1. Log in to WebLogic Administration console:

   ```
   http://<admin server host>:<admin server port>/console
   ```

2. Under Domain Structure, click **Deployments**.
3. Select **oinav (11.1.1.3.0)** from the **Name** table.

4. Click **Update** and click **Finish** in the **Update Application Assistant** screen after verifying the source path.

> **Note:** If WebLogic is running in production mode, click **Lock & Edit** before clicking **Update.**

### Using WebLogic Scripting Tool (WLST)

Complete the following steps to upgrade Oracle Identity Navigator through the WLST console:

### On UNIX

1. Move from your present working directory to the `<MW_HOME>/wlserver_10.3/common/bin` directory by running the following command on the command line:

   ```
   cd <MW_HOME>/wlserver_10.3/common/bin
   ```

2. Run the following command to launch the WebLogic Scripting Tool (WLST):

   ```
   ./wlst.sh
   ```

3. Connect to the Administration Server using the following command:

   connect('weblogic-username','weblogic-password','weblogic-url')

4. At the WLST prompt, run the following command:

   ```
   redeploy('oinav#11.1.1.3.0')
   ```

5. Exit the WLST console using the `exit()` command.

### On Windows

1. Move from your present working directory to the `<MW_HOME>\wlserver_10.3\common\bin` directory by running the following command on the command line:

   ```
   cd <MW_HOME>\wlserver_10.3\common\bin
   ```

2. Run the following command to launch the WebLogic Scripting Tool (WLST):

   ```
   wlst.cmd
   ```

3. Connect to the Administration Server using the following command:

   connect('weblogic-username','weblogic-password','weblogic-url')

4. At the WLST prompt, run the following command:

   ```
   redeploy('oinav#11.1.1.3.0')
   ```

5. Exit the WLST console using the `exit()` command.

## 8.13 Importing the Oracle Identity Navigator 11.1.2 Metadata

You must import the metadata which was exported earlier so that Oracle Identity Navigator gets back the metadata present before upgrade. Import Oracle Identity Navigator 11.1.2 metadata by running the following WLST command:

**On UNIX:**

1. Move from your present working directory to the `<IAM_HOME>/common/bin` directory by running the following command on the command line:

   ```
   cd <IAM_HOME>/common/bin
   ```

2. Run the following command to launch the WebLogic Scripting Tool (WLST):

   ```
   ./wlst.sh
   ```

3. Connect to the Administration Server using the following command:

   ```
   connect('weblogic-username','weblogic-password','weblogic-url')
   ```

4. At the WLST prompt, run the following WLST (online) command:

   ```
   importMetadata(application='oinav',server='AdminServer',fromLocation='e
   xport_directory')
   ```

   where

   `export_directory` is the directory where you have exported the Oracle Identity Navigator metadata to.

**On Windows:**

1. Move from your present working directory to the `<IAM_HOME>\common\bin` directory by running the following command on the command line:

   ```
   cd <IAM_HOME>\common\bin
   ```

2. Run the following command to launch the WebLogic Scripting Tool (WLST):

   ```
   wlst.cmd
   ```

3. Connect to the Administration Server using the following command:

   ```
   connect('weblogic-username','weblogic-password','weblogic-url')
   ```

4. At the WLST prompt, run the following WLST (online) command:

   ```
   importMetadata(application='oinav',server='AdminServer',fromLocation='e
   xport_directory')
   ```

   where

   `export_directory` is the directory where you have exported Oracle Identity Navigator metadata to.

> **Note:** Oracle Business Intelligence Publisher 10*g* report format is not supported in Oracle Identity Navigator 11.1.2 release. It is not mandatory, but if you want to remove the reports, see "Configuring Oracle Business Intelligence Publisher" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Navigator*.

## 8.14 Verifying the Upgrade

To verify the Oracle Identity Navigator upgrade, do the following:

1. Log in to the OINAV console:

   ```
   http://<admin server host>:<admin server port>/oinav
   ```

2. In the Dashboard page, check for the version number in the bottom right corner.

   The version number should be 11.1.2.0.0.

9

# Upgrading Oracle Identity and Access Management 11*g* Release1 (11.1.1.3.0) Environments

This chapter describes how to upgrade Oracle Identity and Access Management 11*g* Release 1 (11.1.1.3.0) environments to Oracle Identity and Access Management 11*g* Release 2 (11.1.2).

Upgrading Oracle Identity and Access Management 11*g* Release 1 (11.1.1.3.0) to Oracle Identity and Access Management 11*g* Release 2 (11.1.2) includes two major tasks:

1. Upgrading Oracle Identity and Access Management 11*g* Release 1 (11.1.1.3.0) to Oracle Identity and Access Management 11*g* Release 1 (11.1.1.5.0)
2. Upgrading Oracle Identity and Access Management 11*g* Release 1 (11.1.1.5.0) to Oracle Identity and Access Management 11*g* Release 2 (11.1.2)

This chapter contains the following sections:

- Overview
- Upgrading Oracle Access Manager 11g Release 1 (11.1.1.3.0)
- Upgrading Oracle Adaptive Access Manager 11g Release 1 (11.1.1.3.0)
- Upgrading Oracle Identity Manager 11g Release 1 (11.1.1.3.0)
- Upgrading Oracle Identity Navigator 11g Release 1 (11.1.1.3.0)

Read the Oracle Fusion Middleware System Requirements and Specifications document to ensure that your environment meets the minimum requirements for the products you are installing or upgrading.

## 9.1 Overview

Before upgrading Oracle Identity and Access Management 11.1.1.3.0 to Oracle Identity and Access Management 11.1.2, you must check if your Oracle Identity and Access Management 11.1.1.3.0 version is supported for upgrade. For more information on the supported starting points for Oracle Identity and Access Management 11.1.1.3.0 upgrade, see Chapter 3, "Upgrade Starting Points".

For more information on upgrade scenarios, see Section 1.2, "Upgrade Scenarios".

## 9.2 Upgrading Oracle Access Manager 11*g* Release 1 (11.1.1.3.0)

To upgrade Oracle Access Manager 11.1.1.3.0 to Oracle Access Management Access Manager 11.1.2, complete the following tasks:

1. Upgrade Oracle Access Manager 11.1.1.3.0 to Oracle Access Manager 11.1.1.5.0

   For more information, see "Updating Oracle Access Manager 11.1.1.3.0 to 11.1.1.5.0" in the *Oracle Fusion Middleware Patching Guide*.

2. Upgrade Oracle Access Manager 11.1.1.5.0 to Oracle Access Management Access Manager 11.1.2

   For more information, see "Chapter 4, "Upgrading Oracle Access Manager 11g Release 1 (11.1.1.5.0) Environments".

## 9.3 Upgrading Oracle Adaptive Access Manager 11*g* Release 1 (11.1.1.3.0)

To upgrade Oracle Adaptive Access Manager 11.1.1.3.0 to Oracle Adaptive Access Manager 11.1.2, complete the following tasks:

1. Upgrade Oracle Adaptive Access Manager 11.1.1.3.0 to Oracle Adaptive Access Manager 11.1.1.5.0

   For more information, see "Updating Oracle Adaptive Access Manager 11.1.1.3.0 to 11.1.1.5.0" in the *Oracle Fusion Middleware Patching Guide*.

2. Upgrade Oracle Adaptive Access Manager 11.1.1.5.0 to Oracle Adaptive Access Manager 11.1.2

   For more information, see "Chapter 5, "Upgrading Oracle Adaptive Access Manager 11g Release 1 (11.1.1.5.0) Environments".

## 9.4 Upgrading Oracle Identity Manager 11*g* Release 1 (11.1.1.3.0)

To upgrade Oracle Identity Management 11.1.1.3.0 to Oracle Identity Management 11.1.2, complete the following tasks:

1. Upgrade Oracle Identity Management 11.1.1.3.0 to Oracle Identity Management 11.1.1.5.0

   For more information, see "Updating Oracle Identity Manager 11.1.1.3.0 to 11.1.1.5.0" in the *Oracle Fusion Middleware Patching Guide.*

2. Upgrade Oracle Identity Management 11.1.1.5.0 to Oracle Identity Management 11.1.2

   For more information, see "Chapter 6, "Upgrading Oracle Identity Manager 11g Release 1 (11.1.1.5.0) Environments".

## 9.5 Upgrading Oracle Identity Navigator 11*g* Release 1 (11.1.1.3.0)

To upgrade Oracle Identity Navigator 11.1.1.3.0 to Oracle Identity Navigator 11.1.2, complete the following tasks:

1. Upgrade Oracle Identity Navigator 11.1.1.3.0 to Oracle Identity Navigator 11.1.1.5.0

   For more information, see "Updating Oracle Identity Navigator 11.1.1.3.0 to 11.1.1.5.0" in the *Oracle Fusion Middleware Patching Guide*.

2. Upgrade Oracle Identity Navigator 11.1.1.5.0 to Oracle Identity Navigator 11.1.2

   For more information, see "Chapter 8, "Upgrading Oracle Identity Navigator 11g Release 1 (11.1.1.5.0) Environments".

# 10

# Upgrading Oracle Identity Manager 9.x Environments

This chapter describes how to upgrade Oracle Identity Manager 9.x to Oracle Identity Manager 11*g* Release 2 (11.1.2). Upgrading Oracle Identity Manager 9.x to Oracle Identity Manager 11.1.2 involves two major tasks:

- Upgrading Oracle Identity Manager 9.x to Oracle Identity Manager 11*g* Release 1 (11.1.1.5.0)
- Upgrading Oracle Identity Manager 11*g* Release 1 (11.1.1.5.0) to Oracle Identity Manager 11*g* Release 2 (11.1.2)

The chapter contains the following sections:

- Overview
- Upgrade Roadmap
- Task 1: Upgrading Oracle Identity Manager 9.x to Oracle Identity Manager 11.1.1.5.0
- Task 2: Upgrading Oracle Identity Manager 11.1.1.5.0 to Oracle Identity Manager 11.1.2

Read the Oracle Fusion Middleware System Requirements and Specifications document to ensure that your environment meets the minimum requirements for the products you are installing or upgrading.

## 10.1 Overview

Before upgrading Oracle Identity Manager 9.x to Oracle Identity Manager 11.1.2, you must check if your Oracle Identity Manager 9.x version is supported for upgrade. For more information on the supported starting points for Oracle Identity Manager 9.x upgrade, see Chapter 3, "Upgrade Starting Points".

For more information on upgrade scenarios, see Section 1.2, "Upgrade Scenarios" in Chapter 1, "Introduction".

## 10.2 Upgrade Roadmap

Table 10–1 lists the steps to upgrade Oracle Identity Manager 9.x to Oracle Identity Manager 11.1.2.

*Table 10–1 Upgrade Flow*

| Task No | Task | For More Information |
|---|---|---|
| 1 | Upgrade your existing Oracle Identity Manager 9.x to Oracle Identity Manager 11.1.1.5.0. | See, Task 1: Upgrading Oracle Identity Manager 9.x to Oracle Identity Manager 11.1.1.5.0 |
| 2 | Upgrade Oracle Identity Manager 11.1.1.5.0 to Oracle Identity Manager 11.1.2.0. | See, Task 2: Upgrading Oracle Identity Manager 11.1.1.5.0 to Oracle Identity Manager 11.1.2 |

## 10.3 Task 1: Upgrading Oracle Identity Manager 9.x to Oracle Identity Manager 11.1.1.5.0

To upgrade Oracle Identity Manager 9.x to Oracle Identity Manager 11.1.1.5.0, refer to "Upgrading Oracle Identity Manager Environment" in the *Oracle Fusion Middleware Upgrade Guide for Oracle Identity Management* in the Oracle Fusion Middleware 11g Release 1 (11.1.1.5.0) documentation library.

## 10.4 Task 2: Upgrading Oracle Identity Manager 11.1.1.5.0 to Oracle Identity Manager 11.1.2

To upgrade Oracle Identity Manager 11.1.1.5.0 to Oracle Identity Manager 11.1.2, refer to Chapter 6, "Upgrading Oracle Identity Manager 11g Release 1 (11.1.1.5.0) Environments".

# Part III

# Migrating Various Oracle 10*g* and OpenSSO Environments

This part includes the following chapters:

# 11

# Migration and Coexistence Starting Points

This chapter outlines the supported starting points for migration and coexistence scenarios. The chapter contains the following sections:

## 11.1 Overview

For more information about migration scenarios, see Section 1.3, "Migration and Coexistence Scenarios".

## 11.2 Supported Starting Points for Oracle Access Manager 10*g* Migration

Table 11–1 lists the releases of Oracle Access Manager 10*g* supported for migration.

***Table 11–1 Oracle Access Manager 10g Releases Supported for Migration***

| Release | Description |
|---|---|
| Oracle Access Manager 10*g* (10.1.4.3) | This version of Oracle Access Manager is supported for migration. |

## 11.3 Supported Starting Points for Oracle Adaptive Access Manager 10*g* Migration

Table 11–2 lists the releases of Oracle Adaptive Access Manager 10*g* supported for migration.

***Table 11–2 Oracle Adaptive Access Manager 10g Releases Supported for Migration***

| Release | Description |
|---|---|
| Oracle Adaptive Access Manager 10*g* (10.1.4.5) | This version of Oracle Adaptive Access Manager was available as a standalone product.<br>Bundle Patch 13 Oracle Adaptive Access Manager 10*g* (10.1.4.5.2) is the latest patchset release for 10*g*. |

## 11.4 Supported Starting Points for Oracle Single Sign-On 10*g* Migration

Table 11–3 lists the releases of Oracle Single Sign-On 10*g* supported for migration.

***Table 11–3 Oracle Single Sign-On 10g Releases Supported for Migration***

| Release | Description |
|---|---|
| Oracle Single Sign-On 10*g* (10.1.2) and 10*g* (10.1.4) | This version of Oracle Single Sign-On was available as part of Oracle Application Server 10*g* Release 2 (10.1.2.3) and 10*g* (10.1.4). |

## 11.5 Supported Starting Points for Sun OpenSSO Enterprise Migration

Table 11–4 lists the releases of Sun OpenSSO Enterprise supported for migration.

***Table 11–4 Sun OpenSSO Enterprise Releases Supported for Migration***

| Release | Description |
|---|---|
| Sun OpenSSO Enterprise 8.0 Update 2 | This version of Sun OpenSSO Enterprise is supported for migration. |

## 11.6 Supported Starting Points for Sun Java System Access Manager Migration

Table 11–5 lists the releases of Sun Java System Access Manager supported for migration.

***Table 11–5 Sun Java System Access Manager Releases Supported for Migration***

| Release | Description |
|---|---|
| Sun Java System Access Manager 7.1 or Sun Java System Access Manager 7.1 Patch 6 | These versions of Sun Java System Access Manager are supported for migration. |

## 11.7 Supported Starting Points for Coexistence of Oracle Access Manager 10*g* With Oracle Access Management Access Manager 11.1.2

Table 11–6 lists the releases of Oracle Access Manager 10*g* supported for coexistence with Oracle Access Management Access Manager 11*g* Release 2 (11.1.2).

*Table 11–6 Oracle Access Manager 10g Releases Supported for Coexistence*

| Release | Description |
|---|---|
| Oracle Access Manager 10*g* (10.1.4.3) | This version with any Bundle Patch is supported for coexistence, where both the Oracle Access Manager 10*g* and Oracle Access Management Access Manager 11*g* Release 2 (11.1.2) deployments coexist. |

## 11.8 Supported Starting Points for Coexistence of Sun OpenSSO Enterprise With Oracle Access Management Access Manager 11.1.2

Table 11–7 lists the releases of Sun OpenSSO Enterprise supported for coexistence with Oracle Access Management Access Manager 11*g* Release 2 (11.1.2).

*Table 11–7 Sun OpenSSO Enterprise Releases Supported for Coexistence*

| Release | Description |
|---|---|
| Sun OpenSSO Enterprise 8.0 Update 2 | This version of Sun OpenSSO Enterprise is supported for coexistence, where both the Sun OpenSSO Enterprise and Oracle Access Management Access Manager 11*g* Release 2 (11.1.2) deployments coexist. |

## 11.9 Supported Starting Points for Coexistence of Sun Java System Access Manager With Oracle Access Management Access Manager 11.1.2

Table 11–8 lists the releases of Sun Java System Access Manager supported for coexistence with Oracle Access Management Access Manager 11*g* Release 2 (11.1.2).

*Table 11–8 Sun Java System Access Manager Releases Supported for Coexistence*

| Release | Description |
|---|---|
| Sun Java System Access Manager 7.1 Patch 6 | This version of Sun Java System Access Manager is supported for coexistence, where both Sun Java System Access Manager and Oracle Access Manager 11*g* deployments coexist. |

# 12

# Migrating Oracle Access Manager 10*g* Environments

This chapter describes how to migrate Oracle Access Manager 10*g* to Oracle Access Management Access Manager (Access Manager) 11*g* Release 2 (11.1.2). The chapter contains the following sections:

## 12.1 Migration Overview

The procedure described in this chapter can be used to migrate the following artifacts of Oracle Access Manager 10*g* to Access Manager 11.1.2.

- Host identifiers
- Agents
- Data stores
- Authentication schemes

- Resource types
- Policy domains

During this migration, you must install Access Manager 11*g* Release 2 (11.1.2), create a new Oracle Home (*IAM_HOME)*, and migrate the policy data from the Oracle Access Manager 10*g* installation to the new Access Manager 11*g* Release 2 (11.1.2) Oracle Home.

This section contains the following topics:

- Modes of Migration
- Migration Summary

## 12.1.1 Modes of Migration

The following are the two modes of migration that you can perform using the procedure described in this chapter:

- Complete Migration
- Incremental Migration

### 12.1.1.1 Complete Migration

This mode of migration migrates all artifacts of Oracle Access Manager 10*g*, which are compatible with 11.1.2, to Access Manager 11.1.2. You can perform complete migration only once. You cannot perform incremental migration after performing complete migration.

### 12.1.1.2 Incremental Migration

Incremental migration is a mode of migration where the selected agents, policy domains and their related artifacts like host identifiers, resource types of the resources, and authentication schemes of Oracle Access Manager 10*g* are migrated to Access Manager 11.1.2. While migrating selected policy domains in incremental migration, the migration utility checks for any dependant artifacts, such as authentication schemes, host identifiers, and resource types; and migrates them first. This migration is followed by the migration of the associated policy domain.

You can migrate the artifacts that are not present in the Access Manager 11.1.2 environment. If an artifact that you wish to migrate is already present in the Access Manager 11.1.2 environment, the artifact is ignored and is not migrated.

You can perform incremental migration for more than once. You can also perform complete migration after incremental migration, or you can migrate all artifacts by performing incremental migration multiple times.

The incremental migration procedure is the same as the complete migration procedure. In addition, you must complete the additional steps required for incremental migration, as described in Additional Steps for Incremental Migration.

## 12.1.2 Migration Summary

Table 12–1 summarizes the artifacts of Oracle Access Manager 10*g* that can be migrated to Access Manager 11.1.2:

***Table 12–1 Compatibility of Artifacts***

| Artifact | Description |
|---|---|
| Host Identifiers | ■ All host identifiers in Oracle Access Manager 10*g* map to a corresponding host identifier in Access Manager 11.1.2.<br>■ Host name variations in Oracle Access Manager 10*g*, which contain non-numeric characters in the port values, are not migrated to Access Manager 11.1.2. Such non-numeric port value is removed, and the host part of the variation is retained.<br>■ Variations duplicated in multiple host identifiers in Oracle Access Manager 10*g* are ignored. If all variations in a given host ID are duplicated, all variations are removed and a new variation is added with the name of the host ID. |
| Agents | ■ All attributes of the Oracle Access Manager 10*g* agent profile are supported in migration except for IIS impersonation user name and password.<br>■ If the Oracle Access Manager 10*g* deployment has a mix of WebGates with `Open/Simple/Cert` transport security mode, the migration utility attempts to migrate WebGate with its transport security mode. In this case, you must configure the Access Manager 11.1.2 server depending to the security mode of the WebGates. For more information, see Section 12.7, "Configuring Transport Security Mode for Access Manager 11.1.2 Server".<br>■ If all WebGates are to be migrated in the same mode, you must set the `agent_mode_to_override` property in the properties file to `OPEN` /`SIMPLE` /`CERT` depending on the mode required. For more information about the properties specified in the properties file, see Table 12–4.<br>■ The migration utility does not generate artifacts like `ObAccessClient.xml`, `password.xml`, `certificates`, as the WebGates already have those artifacts from the Oracle Access Manager 10*g* deployment. If required, you can generate those artifacts by updating the WebGate profile manually using the Access Manager 11.1.2 administration console. |
| Data Stores | ■ Directory instances of Oracle Access Manager 10*g* directory profiles are supported for migration. All relevant attributes of directory instances are migrated and mapped to corresponding data store of Access Manager 11.1.2. If the directory profile contains a secondary directory instance, it is migrated as a separate data store.<br>■ Data stores must be up and running during the migration process. Offline data stores are ignored. |
| Authentication Schemes | ■ Migration of authentication schemes like Form, Basic, and X509 is supported.<br>■ Migration of authentication schemes with customized authentication flows is also supported.<br>■ Authentication schemes with custom authentication challenge parameters are migrated without the custom challenge parameters. After migration, you must manually add or change the challenge parameters in the migrated authentication schemes with the same values used in the corresponding Oracle Access Manager 10*g* authentication schemes.<br>■ External authentication schemes from Oracle Access Manager 10*g* are not supported in Access Manager 11.1.2. Therefore, external authentication schemes are migrated to 11.1.2 using Delegated Authentication Protocol (DAP). The migrated scheme requires some post-migration steps.<br>■ Migration of custom authentication is not supported. If an authentication scheme contains custom plug-ins, such schemes may not be migrated correctly.<br>■ All authentication schemes of type **Anonymous** in Oracle Access Manager 10*g* are directly mapped to one single Authentication scheme **NONE** in Access Manager 11.1.2. |

*Table 12–1 (Cont.) Compatibility of Artifacts*

| Artifact | Description |
|---|---|
| Resource Types | ■ Oracle Access Manager 10*g* resource types and the migrated Access Manager 11.1.2 resources types have one-to-one mapping.<br>■ Resource types with name **HTTP**, **wl_authen** are not migrated, as they are available out-of-the-box in Access Manager 11.1.2. |

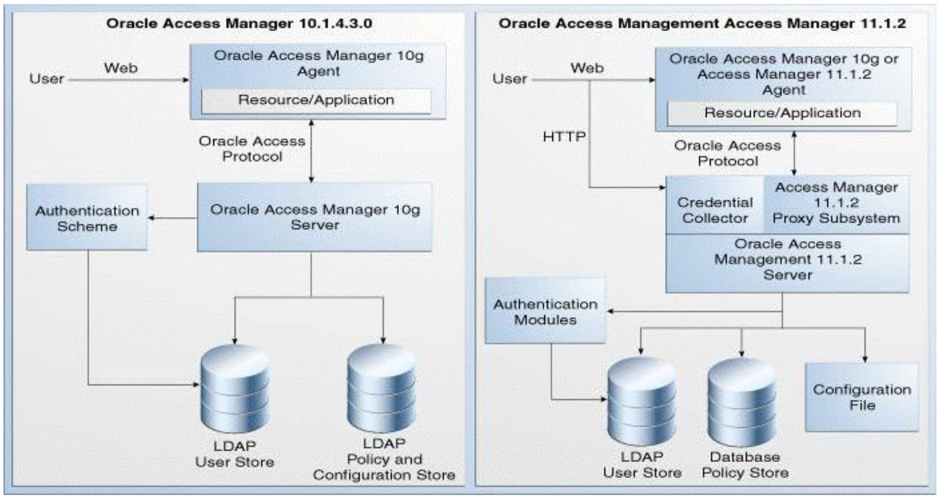
*Table 12–1 (Cont.) Compatibility of Artifacts*

| Artifact | Description |
|---|---|
| Policy Domains | ■ Policy domains of Oracle Access Manager 10*g* map to a distinct application domain in Access Manager 11.1.2.<br>■ URL prefixes are migrated to Access Manager 11.1.2. For every prefix, an additional resource `<urlprefix>/**` is created and protected by default authentication and authorization policies. If any of the internal policies contain URL prefixes with all operations selected and without any URL Pattern, then the resources `<urlprefix>` and `<urlprefix>/**` are removed from the default authentication scheme. The resources are protected by the authentication scheme configured for that particular internal policy. Such resource is created by selecting all of the operations defined in its resource type.<br>■ The default authentication rule and the authorization expression is migrated to the default authentication and authorization policy, respectively.<br>■ Only success/failure responses and redirects associated with authorization expressions are supported for migration. Inconclusive responses and redirects are ignored. Responses and redirects associated with authorization rules are not considered for migration because Access Manager 11.1.2 does not support them. For authentication rules, both the success and failure redirects and responses are migrated to Access Manager 11.1.2. However, in the user interface, only success responses are displayed.<br>■ Authorization rules that do not form part of any authorization expression are ignored during migration.<br>■ While migrating Oracle Access Manager 10*g* internal policies to Access Manager 11.1.2:<br>    ■ If the authentication rule is using the default authentication rule associated with the policy domain, resources defined in the internal policy are associated with the default authentication policy after the migration. Otherwise, a new authentication policy is created for the authentication rule.<br>    ■ If the authorization expression is using the default authorization expression associated with the policy domain, resources defined in the internal policy are associated with the default authorization policy after migration. Otherwise, a new authorization policy is created for the authorization expression.<br>    ■ In Oracle Access Manager 10*g*, ALLOW and DENY conditions associated with an authorization rule taking part in the expression are converted into conditions during migration. Later ALLOW and DENY rules are created for the migrated authorization policy using the migrated conditions.<br>    ■ Timing conditions are migrated as temporal conditions, and they form part of the ALLOW or DENY rule in Access Manager 11.1.2.<br>    ■ After migration, only ALLOW rule is created, which will have a combined expression containing ALLOW and DENY conditions such that the evaluation results in ALLOW or DENY. DENY rule will always be empty. |

## 12.2 Topology Comparison

Figure 12–1 compares the topologies of Oracle Access Manager 10g and Access Manager 11.1.2.

***Figure 12–1 Comparison of Oracle Access Manager 10g and Access Manager 11.1.2 Topologies***


Oracle Access Manager 10.1.4.3.0
User
Web
Oracle Access Manager 10g Agent
Resource/Application
Oracle Access Protocol
Authentication Scheme
Oracle Access Manager 10g Server
LDAP User Store
LDAP Policy and Configuration Store
Oracle Access Management Access Manager 11.1.2
User
Web
HTTP
Oracle Access Manager 10g or Access Manager 11.1.2 Agent
Resource/Application
Oracle Access Protocol
Credential Collector
Access Manager 11.1.2 Proxy Subsystem
Oracle Access Management 11.1.2 Server
Authentication Modules
LDAP User Store
Database Policy Store
Configuration File

## 12.3 Migration Roadmap

Table 12–2 lists the steps to migrate Oracle Access Manager 10*g* to Access Manager 11.1.2.

***Table 12–2 Migration Tasks***

| Task No | Task | For More Information |
|---|---|---|
| 1 | Complete the prerequisites. | See, Prerequisites for Migration |
| 2 | Install Oracle Identity and Access Management 11*g* Release 2 (11.1.2). | See, Installing Oracle Identity and Access Management 11.1.2 |
| 3 | Configure Access Manager 11.1.2. | See, Configuring Oracle Access Management Access Manager 11.1.2 |
| 4 | Configure the security mode of the Access Manager 11.1.2 server instance and the WebGates, so that the Access Manager 11.1.2 server accepts connections from the agents when WebGates start communicating with Access Manager 11.1.2 after migration. | See, Configuring Transport Security Mode for Access Manager 11.1.2 Server |
| 5 | Start the Administration Server and the Access Manager 11.1.2 Managed Servers. | See, Starting Administration Server and Access Manager 11.1.2 Managed Servers |

*Table 12–2 (Cont.) Migration Tasks*

| Task No | Task | For More Information |
|---|---|---|
| 6 | Create a properties file with the LDAP details and the required information. | See, Creating a Properties File |
| 7 | Generate the assessment report, and analyze what agents and artifacts can be migrated to Access Manager 11.1.2.<br>You can perform this task multiple times before you migrate your Oracle Access Manager 10*g* environment. | See, Generating the Assessment Report |
| 8 | Restart the Administration Server for the domain that has Access Manager 11.1.2. | See, Restarting the Administration Server |
| 9 | If you wish to perform incremental migration, complete the additional steps (for example, creating an input file).<br>Ignore this task if you wish to perform complete migration. | See, Additional Steps for Incremental Migration |
| 10 | Migrate Oracle Access Manager 10*g* to Access Manager 11.1.2. | See, Migrating the Artifacts of Oracle Access Manager 10g to Access Manager 11.1.2 |
| 11 | If you are using 10*g* WebGates with Access Manager 11.1.2, you must configure the centralized logout for 10*g* WebGates to work with Access Manager 11.1.2 server. | See, Configuring Centralized Logout for 10g WebGates with Access Manager 11.1.2 |
| 12 | Associate the migrated WebGates with the Oracle Access Management 11.1.2 Server. | See, Associating the WebGates with Access Manager 11.1.2 Server |
| 13 | Verify the migration. | See, Verifying the Migration |

## 12.4 Prerequisites for Migration

You must complete the following prerequisites for migrating Oracle Access Manager 10*g* to Access Manager 11.1.2:

1. Read the Oracle Fusion Middleware System Requirements and Specifications document to ensure that your environment meets the minimum requirements for the products you are installing, upgrading, and migrating.

**Note:** For information about Oracle Fusion Middleware concepts and directory structure, see "Understanding Oracle Fusion Middleware Concepts and Directory Structure" in the *Oracle Fusion Middleware Installation Planning Guide for Oracle Identity and Access Management*.

2. Verify that the Oracle Access Manager 10*g* version that you are using is supported for migration. For information about supported starting points for Oracle Access Manager 10*g* migration, see Section 11.2, "Supported Starting Points for Oracle Access Manager 10g Migration".
3. Make sure that all the user stores configured in your Oracle Access Manager 10*g* deployment are running.

**Note:** The migration utility does not support connections with the configuration store over SSL port.

## 12.5 Installing Oracle Identity and Access Management 11.1.2

As part of the migration process, you must install Oracle Identity and Access Management 11*g* Release 2 (11.1.2). Oracle Identity and Access Management is a suite that contains Oracle Access Management Access Manager 11.1.2. This installation can be on the same machine where Oracle Access Manager 10*g* is installed, or on a different machine.

For more information about installing Oracle Identity and Access Management 11.1.2, see "Installing Oracle Identity and Access Management (11.1.2)" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

## 12.6 Configuring Oracle Access Management Access Manager 11.1.2

After installing Oracle Identity and Access Management 11.1.2, you must configure Access Manager 11.1.2, and create a domain.

For information about configuring Access Manager 11.1.2, see "Configuring Oracle Access Management" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

## 12.7 Configuring Transport Security Mode for Access Manager 11.1.2 Server

You must configure the security mode of the Access Manager 11.1.2 Server, so that the migrated WebGates communicate with the Access Manager 11.1.2 Server after migration. The following are the security modes listed in the increasing order of their security level:

- `Open`
- `Simple`
- `Cert`

`Open` is the least secured mode, and `Cert` is the most secured mode. `Open` is the default security mode. The security mode in which the Access Manager 11.1.2 server must be configured depends on the security modes of the Oracle Access Manager 10*g* WebGates that you wish to migrate.

This section contains the following topics:

- Deciding the Security Mode of Access Manager 11.1.2 Server
- Configuring Cert Mode Communication for Access Manager 11.1.2 Server
- Configuring Simple Mode Communication for Access Manager 11.1.2 Server

### 12.7.1 Deciding the Security Mode of Access Manager 11.1.2 Server

If all the WebGates that you migrate have the same security mode, you must configure the Access Manager 11.1.2 Server in the respective modes. If you have mix of migrated WebGates configured in different security modes, you must configure the Access Manager 11.1.2 Server in the mode with the lower security level. Table 12–3 lists the various use cases and the security mode in which you must configure the Access Manager 11.1.2 Server.

***Table 12–3 Choosing the Security Mode for Access Manager 11.1.2 Server***

| Transport Security Mode of Oracle Access Manager 10*g* WebGates | Security Mode to be Configured for Access Manager 11.1.2 Instance | Configuration Procedure |
|---|---|---|
| Some or all `Open` | `Open` | `Open` mode is the default mode. No additional steps are necessary. |
| All `Cert` | `Cert` | See Configuring Cert Mode Communication for Access Manager 11.1.2 Server. |
| All `Simple` | `Simple` | See Configuring Simple Mode Communication for Access Manager 11.1.2 Server. |
| Mix of `Open`, `Simple`, and `Cert` | `Open` | `Open` mode is the default mode. No additional steps are necessary. |
| Mix of `Simple` and `Cert` | `Simple` | See Configuring Simple Mode Communication for Access Manager 11.1.2 Server. |

### 12.7.2 Configuring Cert Mode Communication for Access Manager 11.1.2 Server

To configure `Cert` mode communication for Access Manager 11.1.2, complete the following tasks in section "Configuring Cert Mode Communication for Access Manager" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*:

1. Reviewing "Introduction to Securing Communication Between OAM Servers and Webgates", and "About Cert Mode Encryption and Files"

   Complete all of the steps described in this task.

2. "Generating a Certificate Request and Private Key for OAM Server"

   Complete all of the steps described in this task.

3. "Retrieving the OAM Keystore Alias and Password"

   Complete all of the steps described in this task.

4. "Importing the Trusted, Signed Certificate Chain Into the Keystore"

In this task, you import the Certificate Authority (CA) certificate used to issue the `Cert` mode certificate for WebGate. If this CA certificate is different from the certificate that is already trusted by the Access Manager 11.1.2 Server, perform the following steps under this task. Otherwise, ignore these tasks.

- "**aaa_chain.pem**: Using a text editor, modify the aaa_chain.pem file to remove all data except that which is contained within the CERTIFICATE blocks, then save the file"
- "Import the trusted certificate chain using the following command with details for your environment"
- "When prompted to trust this certificate, type **yes**"

5. "Adding Certificate Details to Access Manager Settings"

   Ignore the step "Open the OAM Server registration page, click the Proxy tab, change the Proxy mode to Cert, and click Apply" under this task.

If the root certificate authority (CA) used for the `Cert` mode certificate of the Access Manager 11.1.2 Server is different from the CA certificate present in `aaa_chain.pem` file on the WebGate side, you must update the `aaa_chain.pem` file with the root CA certificate used to issue the server `Cert` mode certificates. To do this, complete the following steps:

1. Obtain the CA certificate in PEM format that was used to generate `Cert` mode certificates for the Access Manager 11.1.2 Server instance.
2. Open this CA certificate in any text editor, copy the content from this file, including the BEGIN, END markers. For example:

   ```
   ----BEGIN CERTIFICATE-----

       ...

       CERTIFICATE

        ...

   -----END CERTIFICATE-----
   ```

3. Open the `aaa_chain.pem` file from the location *`OHS_INSTANCE_HOME`*`/config/OHS/ohs2/webgate/config` using any text editor, and paste the content of server CA certification base 64 encoded contents to the end of the `aaa_chain.pem` file.
4. Save the file, and close.

### 12.7.3 Configuring Simple Mode Communication for Access Manager 11.1.2 Server

To configure `Simple` mode communication for the Access Manager 11.1.2 Server, complete the following steps:

1. Log in to the Oracle Access Management 11.1.2 Administration console, using the following URL:

   ```
   http://<host>:<port>/oamconsole
   ```

   where `<host>` is the machine on which Access Manager 11.1.2 is running, and `<port>` is the port number.
2. Go to the **System Configuration** tab.
3. Expand **Access Manager**, and double-click **Access Manager Settings**.
4. Expand the **Access Protocol** section.

5. Set **Global Passphrase** to the same value used in your Oracle Access Manager 10*g* deployment.

## 12.8 Starting Administration Server and Access Manager 11.1.2 Managed Servers

Before you start migrating Oracle Access Manager 10*g* to Access Manager 11.1.2, make sure that the WebLogic Administration Server and the Access Manager 11.1.2 Managed Servers are up and running before you start migrating Oracle Access Manager 10*g*. If you have not started the WebLogic Administration Server and the Access Manager 11.1.2 Managed Servers, start them using the following procedure:

### Starting Administration Server

To start the Administration Server, do the following:

**On UNIX**:

1. Move from your present working directory to the directory `*MW_HOME*/user_projects/domains/*domain_name*/bin` using the command:

   ```
   cd MW_HOME/user_projects/domains/domain_name/bin/
   ```

2. Run the following command:

   ```
   ./startWebLogic.sh
   ```

   When prompted, enter the WebLogic Administration Server username and password.

**On Windows**:

1. Move from your present working directory to the directory `*MW_HOME*\user_projects\domains\*domain_name*\bin` using the following command on the command line:

   ```
   cd MW_HOME\user_projects\domains\domain_name\bin\
   ```

2. Run the following command:

   ```
   startWebLogic.cmd
   ```

   When prompted, enter the WebLogic Administration Server username and password.

### Starting Access Manager 11.1.2 Managed Servers

To start a Access Manager 11.1.2 Managed Server, do the following:

**On UNIX**:

1. Move from your present working directory to the directory `*MW_HOME*/user_projects/domains/*domain_name*/bin` using the command:

   ```
   cd MW_HOME/user_projects/domains/domain_name/bin/
   ```

2. Run the following command:

   ```
   ./startManagedWebLogic.sh oam_managed_server admin_url
   ```

   In this command,

*oam_managed_server* is the name of the Access Manager 11.1.2 Managed Server to be started.

*admin_url* is the URL of the WebLogic administration console. It must be specified in the format `http://`*host*`:`*port*`/console`.

When prompted, enter the WebLogic Administration Server username and password

**On Windows**:

1. Move from your present working directory to the directory *MW_HOME*`\user_projects\domains\`*domain_name*`\bin` using the following command on the command line:

   ```
   cd MW_HOME\user_projects\domains\domain_name\bin\
   ```

2. Run the following command:

   ```
   startManagedWebLogic.cmd oam_managed_server admin_url
   ```

   In this command,

   *oam_managed_server* is the name of the Access Manager 11.1.2 Managed Server to be started.

   *admin_url* is the URL of the administration console. It must be specified in the format `http://`*host*`:`*port*`/console`.

   When prompted, enter the WebLogic Administration Server username and password.

## 12.9 Creating a Properties File

Create a properties file in any accessible location. For example, create an `oam_migration.properties` file.

The content of the properties file should be the following:

```
## Configuration store details
config_store_ldap_url=ldap://<Host Name>:<Port>/
config_store_ldap_base=<Configuration store ldap base>
config_store_principal=<Configuration store LDAP Principal>
config_store_password=<Configuration store OAM 10g encrypted password>
config_store_initial_context_factory=com.sun.jndi.ldap.LdapCtxFactory

## Policy store details
policy_store_ldap_url=ldap://<Host Name>:<Port>/
policy_store_ldap_base=<Policy store ldap base>
policy_store_principal=<Policy store LDAP Principal>
policy_store_password=<Policy store OAM 10g encrypted password>
policy_store_initial_context_factory=com.sun.jndi.ldap.LdapCtxFactory

## migration_mode indicates what type of migration does the administrator intends
## to perform.
## 1. COMPLETE   : A full migration will be performed. Ideal for a new OAM 11g
##                 environment with a clean database.
## 2. INCREMENTAL: In case complete migration has already been performed and
##                 optimizations are done in the 10g environment, then
##                 incremental mode can be used to migrate selective artifacts
##                 from 10g enviroment. Incremental mode will be dictated by the
##                 include and exclude file properties.
## Defaults to COMPLETE if not specified.
```

```
migration_mode=COMPLETE

## The include filename property indicates the absolute filename that would
## contain the list of artifacts that the administration wishes to selectively
## migrate to the 11g environment in incremental mode. For migration modes other
## than incremental, this property will be directly ignored.
include_file=<include input filename>

## The exclude filename property indicates the absolute filename that would
## contain the list of artifacts that the administration wishes to selectively
## exclude from migrating to the 11g environment in incremental mode. For
## migration modes other than incremental, this property will be directly ignored.
## In incremental mode migration, if the administrator specifies both the include
## and exclude files then the include file wiil take precedence and exclude file
## will be ignored.
exclude_file=<exclude input filename>

## This flag denotes whether the preview file should be created or not. If true,
## then preview report will be created irrespective of the value of the
## evaluate_only flag. If set to false, then preview report will not be created.
## Defaults to TRUE if not specified.
preview_enabled=true

## Parameter to filter out preview report file based on the compatibility of an
## artifact. It can take values as COMPATIBLE, INCOMPATIBLE and ALL.
## If set to INCOMPATIBLE, it will include records with compatibility as
## INCOMPATIBLE,INCOMPATIBLE_WITH_LESS_FEATURES and IGNORE. If set to COMPATIBLE,
## it will include records with compatibility as COMPATIBLE. If set to ALL,
## it will include all types of record.
## Defaults to INCOMPATIBLE if not specified.
preview_level=ALL

## Indicates the absolute path and filename of the evaluation preview record file.
## If not specified, defaults to
## <MW_Home>/user_projects/domains/base_domain/MigrationPreviewFile.txt
evaluate_filename=<Preview report filename>

## Flag indicating whether the migration utility runs in evalute mode. If true,
## only preview records will be generated and actual migration to 11g environment
## will be skipped. If false, then actual migration will take place.
## Defaults to FALSE if not specified.
evaluate_only=false

## Parameter for indicating the threashold limit for the artifacts processed in
## memory. Can be used on machines with less memory. If not provided, then
## defaults to 5000. If the migration utility is being used in 'evaluate only'
## mode, this value will be ignored.
## If you feel that the memory will not prove to be insufficient for the amount
## of data that is being migrated, set the value to "MAX".
artifact_queue_limit=3000

## Parameter to provide mode of an agent while migration. It will migrate all the
## agents in the mode specified here. The values can be, OPEN, SIMPLE, CERT
## and RETAIN_EXISTING. Defualt value will be RETAIN_EXISTING. This value will
## migrate agent in its existing mode.
agent_mode_to_override=RETAIN_EXISTING
```

Table 12–4 describes the values you must provide for each of the properties in the properties file.

***Table 12–4 Property File Values***

| Property | Description |
|---|---|
| `config_store_ldap_url` | Specify the LDAP host and the port of the configuration store used in Oracle Access Manager 10*g* deployment in the format: `ldap://<hostname>:<port>` |
| `config_store_ldap_base` | Specify the LDAP search base for the configuration store of the Oracle Access Manager 10*g* deployment. This is the same search base that you provided during the installation of Oracle Access Manager 10*g*. To get this value, do the following:<br>**1.** Log in to the Oracle Access Manager 10*g* Administration console.<br>**2.** Go to the **System Configuration** tab.<br>**3.** Click **Server settings** on the left navigation pane.<br>**4.** Check for the value displayed for **Configuration Base**. Use the parent node of `oblix`.<br>For example, if the **Configuration Base** value displayed on the console is **o=Oblix,dc=company,dc=us**, then the value for this property `configuration_store_ldap_base` must be `dc=company,dc=us`. |
| `config_store_principal` | Specify the LDAP DN of the administrator for the configuration store. |
| `config_store_password` | Specify the encrypted password of the Oracle Access Manager 10*g* configuration LDAP store. To get the encrypted password, do the following:<br>**1.** Move from your present working directory to the location:<br>*`Access_Server_Installation Directory`*`/oblix/config/ldap/`<br>**2.** Copy the value of `ldapRootPasswd` from the `ConfigDB.xml` file.<br>**3.** Use this value for the `config_store_password` property in the properties file. |
| `config_store_initial_ context_factory` | The value of this property must be `com.sun.jndi.ldap.LdapCtxFactory`. Do not modify this value. |
| `policy_store_ldap_url` | Specify the LDAP host and the port of the policy store used in Oracle Access Manager 10*g* deployment in the format: `ldap://<hostname>:<port>`. |
| `policy_store_ldap_base` | Specify the LDAP search base for the policy store of the Oracle Access Manager 10*g* deployment. This is the same search base that you provided during the installation of Oracle Access Manager 10*g*. To get this value, do the following:<br>**1.** Log in to the Oracle Access Manager 10*g* Administration console.<br>**2.** Go to the **System Configuration** tab.<br>**3.** Click **Server settings** on the left navigation pane.<br>**4.** Check for the value displayed for **Policy Base**. Use the parent node of `oblix`.<br>For example, if the **Policy Base** value displayed on the console is **o=Oblix,dc=company,dc=us**, then the value for this property `policy_store_ldap_base` must be `dc=company,dc=us`. |
| `policy_store_principal` | Specify the LDAP DN of the administrator for the policy store. |

*Table 12–4 (Cont.) Property File Values*

| Property | Description |
|---|---|
| policy_store_password | Specify the encrypted password of the Oracle Access Manager 10*g* policy LDAP store. To get the encrypted password, do the following:<br>1. Move from your present working directory to the location:<br>*Access_Server_Installation_Directory*/oblix/config/ldap/<br>2. Copy the value of ldapRootPasswd from the WebResrcDB.xml file.<br>3. Use this value for the policy_store_password property in the properties file. |
| policy_store_initial_<br>context_factory | The value of this property must be com.sun.jndi.ldap.LdapCtxFactory. Do not modify this value. |
| migration_mode | This property indicates the mode of migration you wish to perform. Set one of the following values:<br>■ COMPLETE<br>Specify this value if you wish to perform complete migration. This is ideal for a new Access Manager 11.1.2 environment with a clean database.<br>■ INCREMENTAL<br>Specify this value if you wish to perform incremental migration.<br>Incremental mode is dictated by the include_file and exclude_file properties that you specify in the properties file.<br>For more information about the modes of migration, see "Modes of Migration". |
| include_file | If you wish to perform incremental migration and migrate some of the artifacts to Access Manager 11.1.2, you must use the include_file property.<br>The value of the include_file property must be the absolute path to the file that contains the list of artifacts that you wish to migrate to Access Manager 11.1.2. For more information about creating an include file, see "Additional Steps for Incremental Migration".<br>If you wish to perform incremental migration with the include_file property, then comment out the exlcude_file property.<br>If you specify both include_file and exclude_file properties when you perform incremental migration, the include_file property takes precedence over exclude_file property, and the exclude_file property is ignored.<br>For complete migration, this property is ignored. |

***Table 12–4 (Cont.) Property File Values***

| Property | Description |
|---|---|
| `exclude_file` | If you wish to perform incremental migration and exclude some of the artifacts from the migration, you must use the `exclude_file` property.<br>The value of the `exclude_file` property must be the absolute path to the file that contains the list of artifacts that you wish to exclude from the migration. For more information about creating an exclude file, see "Additional Steps for Incremental Migration".<br>If you wish to perform incremental migration with the `exclude_file` property, then comment out the `inlcude_file` property.<br>If you specify both `include_file` and `exclude_file` properties when you perform incremental migration, `include_file` property takes precedence over `exclude_file` property, and the `exclude_file` property is ignored.<br>For complete migration, this property is ignored. |
| `preview_enabled` | This property indicates whether the assessment report should be created. If the value of this property is set to `true`, the assessment report is generated irrespective of the value of the `evaluate_only` property.<br>If the value of the `preview_enabled` property is set to `false`, the assessment report is not generated.<br>If you do not specify any value, the default value `true` is used and the assessment report is generated. |
| `preview_level` | This property filters the data in the assessment report based on the compatibility of an artifact. You can provide one of the following values for this property:<br>■ `COMPATIBLE`<br>■ `INCOMPATIBLE`<br>■ `ALL`<br>If the value of this property is set to `COMPATIBLE`, the assessment report includes the artifacts of Oracle Access Manager 10*g* that are compatible in Access Manager 11.1.2.<br>If the value of this property is set to `INCOMPATIBLE`, the assessment report includes the artifacts of Oracle Access Manager 10*g* that are incompatible in Access Manager 11.1.2, compatible with less features in Access Manager 11.1.2, and the artifacts that are ignored in Access Manager 11.1.2.<br>If the value of this property is set to `ALL`, the assessment report contains artifacts of Oracle Access Manager 10*g* that are compatible in Access Manager 11.1.2, incompatible in Access Manager 11.1.2, compatible with less features in Access Manager 11.1.2, and the artifacts that are ignored in Access Manager 11.1.2.<br>For more information about the artifacts that are incompatible, and compatible with less features, see Table 12–6. |
| `evaluate_filename` | You must provide the absolute path and the filename for the assessment report file that you wish to generate. The default path is *`MW_HOME`*`/user_projects/domains/base_domain/MigrationPreviewFile.txt`, and the default name of the assessment report is `MigrationPreviewFile.txt`. |

*Table 12–4 (Cont.) Property File Values*

| Property | Description |
|---|---|
| `evaluate_only` | This properties indicates if the migration utility is run in evaluate mode.<br>If the value of this property is set to `true`, only the assessment report is generated, and Oracle Access Manager 10*g* is not migrated to Access Manager 11.1.2.<br>If the value of this property is set to `false`, the assessment report is generated, and Oracle Access Manager 10*g* is migrated to Access Manager 11.1.2.<br>If you do not specify any value to this property, the default value `false` is used. |
| `artifact_queue_limit` | This property indicates the threshold limit for the artifacts processed in memory. This property can be specified when you are using machines with less memory for the migration process.<br>If the amount of data that is migrated is more, and the memory is sufficient, set the value of this property to `MAX`.<br>The default value of this property is `5000`. If the migration utility is run in evaluate mode, the value of this property is ignored. |
| `agent_mode_to_override` | This property indicates the mode in which all agents are migrated. You can specify one of the following values to this property:<br>■ `OPEN`<br>Specify this value if you wish to migrate all the agents in `OPEN` mode.<br>■ `SIMpLE`<br>Specify this value if you wish to migrate all the agents in `SIMPLE` mode.<br>■ `CERT`<br>Specify this value if you wish to migrate all the agents in `CERT` mode.<br>■ `RETAIN_EXISTING`<br>Specify this value if you wish to migrate the agents in their existing modes.<br>The default value is `RETAIN_EXISTING`. |

**Note:** The value for the `config_store_password` property must be encrypted. You can obtain the encrypted password from *`10g_Installation_Directory`*`/Access/oblix/config/ldap/ConfigDB.xml` file.

The value for the `policy_store_password` property must be encrypted. You can obtain the encrypted password from *`10g_Installation_Directory`*`/Access/oblix/config/ldap/WebResrcDB.xml` file.

## 12.10 Generating the Assessment Report

You should generate an assessment report before you can migrate the Oracle Access Manager 10*g* artifacts to Access Manager 11.1.2.

An assessment report is a text file generated when you run the migration utility by setting the appropriate properties in the properties file. The assessment report is generated at the location specified for the property `evaluate_filename` in the properties file.

This report contains the information about all the artifacts in Oracle Access Manager 10*g* along with the information about their compatibility in Access Manager 11.1.2.

This report contains three sections of data:

1. Notes about how to analyze the report, and some generic information about the compatibility of the artifacts.
2. Number of artifacts that are compatible, incompatible, compatible with less features, and ignored in Access Manager 11.1.2
3. Detailed information about all the artifacts of Oracle Access Manager 10*g* in a tabular format.

Table 12–5 lists the columns of the table, which displays information about the artifacts of Oracle Access Manager 10*g*:

***Table 12–5 Assessment Report Content***

| Column No | Column | Description |
|---|---|---|
| 1 | **ARTIFACT TYPE** | This column displays the type of the artifact in Oracle Access Manager 10*g*. The following are the types of artifacts:<br>■ DATA SOURCES<br>■ AUTHENTICATION SCHEMES<br>■ RESOURCE TYPES<br>■ HOST IDs<br>■ AGENTS<br>■ POLICY DOMAINS |
| 2 | **ARTIFACT** | This column lists the names of all the artifacts of Oracle Access Manager 10*g*.<br>The name of the policy domain is divided into two parts. The first part indicates the name of the policy domain, and the second part indicates the content of the policy domain. |
| 3 | **DETAILS** | This column displays information about each of the artifacts.<br>■ For the artifact type **DATA SOURCES**, the name, host and port are listed here.<br>■ For the artifact type **AUTHENTICATION SCHEMES**, a description of each of the artifacts is displayed.<br>■ For the artifact type **RESOURCE TYPES**, the details of the artifact are displayed, if any.<br>■ For the artifacts type **HOST IDs**, the host and the port of each artifact is displayed.<br>■ For the artifacts type **AGENTS**, the mode of the artifact is displayed.<br>■ For the artifact type **POLICY DOMAINS**, the name of the policy domain is displayed. |

*Table 12–5 (Cont.) Assessment Report Content*

| Column No | Column | Description |
|---|---|---|
| 4 | **COMPATIBILITY** | This column displays information about the compatibility of artifacts in Access Manager 11.1.2.if the artifact is compatible with Access Manager 11.1.2 or not. The value for every artifact in this column can be one of the following:<br>■ **COMPATIBLE**: This indicates that the artifact is supported in Access Manager 11.1.2 and the migration utility does not perform any additional modelling.<br>■ **INCOMPATIBLE**: This indicates that the artifact is not supported in Access Manager 11.1.2, and will not be migrated.<br>■ **COMPATIBLE_WITH_LESS_FEATURES**: This indicates that the artifact is compatible in Access Manager 11.1.2, but with less features. The migration utility performs some modelling in order to map this artifact to 11.1.2. All the artifacts with this compatibility mode are migrated.<br>■ **IGNORE**: This indicates that the artifact is not useful in Access Manager 11.1.2, and hence will be ignored while migration. |
| 5 | **MESSAGE** | This column displays any message relevant to the migration of the respective artifact. |
| 6 | **ACTION REQUIRED** | This column displays the action required by the user, if any. |

**Note:** The level of data generated by the assessment report is determined by the property `preview_level` in the properties file.

You can generate the assessment report multiple times before you can actually migrate the artifacts of Oracle Access Manager 10*g* to Access Manager 11.1.2.

Table 12–6 shows the types of artifacts of Oracle Access Manager 10*g* that are incompatible and compatible with less features in Access Manager 11.1.2.

*Table 12–6 Assessment Reports Summary*

| Artifacts | Description |
|---|---|
| **INCOMPATIBLE** | ■ Policy domains that contain URL prefixes for heterogeneous resource types are incompatible with the Access Manager 11.1.2 environment.<br>■ Operation **OTHER** for type HTTP is incompatible with Access Manager 11.1.2, and is not migrated.<br>■ Delegated administration rights associated with policy domains are not considered for migration.<br>■ WebGate profile names greater than 255 characters are not migrated.<br>■ Authentication schemes containing custom authentication plug-ins are not migrated. |

*Table 12–6 (Cont.) Assessment Reports Summary*

| Artifacts | Description |
|---|---|
| **COMPATIBLE_WITH_LESS_FEATURES** | ■ Resources that are identified as `IGNORE` in the policy domain are marked as `COMPATIBLE_WITH_LESS_FEATURES`.<br>■ Access Manager 11.1.2 supports specifying either **query string pattern** or **query name-value** pairs. During migration, if a policy has both query string and query name-value pairs, only query string is migrated.<br>■ External authentication schemes such as DAP are not supported.<br>■ If the host name variation is in the incorrect format or the port value is non-numeric, the host identifier is marked as `COMPATIBLE_WITH_LESS_FEATURES`.<br>■ If host name variation exists in some other host identifier, it is removed from the host identifier and is marked as `COMPATIBLE_WITH_LESS_FEATURES`.<br>■ Timing conditions like **Time of the Day** and **Day of the Week** from the authorization rules in Oracle Access Manager 10*g* policy domain are migrated to Access Manager 11.1.2. The other conditions such as **Months of the Year** and **Days of the Month** are not supported in Access Manager 11.1.2, so they are not migrated.<br>■ Artifacts with names exceeding 255 characters, and description exceeding 1024 characters are migrated with less features. The migration utility truncates the name of the artifact if its name exceeds 255 characters, and adds this truncated name to the beginning of the description. If the description of an artifact exceeds 1024 characters, the extra characters are lost during migration. |

To generate the assessment report, do the following:

1. Edit the properties file that you created in Section 12.9, "Creating a Properties File" as follows:

    1. Set the value of the `migration_mode` property to `COMPLETE`.

    2. Set the value of the `preview_enabled` property to `true`.

    3. Set the value of the `evaluate_only` property to `true`.

    4. Make sure that you have set the absolute path of the assessment report file to the `evaluate_filename` property.

    5. Save the properties file, and close.

2. Perform step-2 to step-6 in the Section 12.13, "Migrating the Artifacts of Oracle Access Manager 10g to Access Manager 11.1.2".

    This generates the assessment report at the location specified by the `evaluate_filename` property in the properties file that you created. You can also open this report in Microsoft Excel. The records included in the assessment report are according to the value set for the `preview_level` property in the properties file.

    Since the `evaluate_only` property in the properties file is set to `true`, the migration utility only generates the assessment report, and it does not migrate the Oracle Access Manager 10*g* artifacts.

> **Note:** You can analyze the evaluation report, and make any necessary changes to the Oracle Access Manager 10*g* environment before proceeding with the migration.

If you wish to generate the assessment report and migrate the Oracle Access Manager 10*g* artifacts, set the value for `evaluate_only` property to `false`, and follow the steps described in Section 12.13, "Migrating the Artifacts of Oracle Access Manager 10g to Access Manager 11.1.2".

> **Note:** When you generate the assessment report, the migration utility also generates a text file called `IncludeFile.txt` at the same location where the assessment report is generated. This file can be used to specify the artifacts that you wish to migrate while performing incremental migration. For more information about using the `IncludeFile.txt` for incremental migration, see "Additional Steps for Incremental Migration".

## 12.11 Restarting the Administration Server

Restart the WebLogic Administration Server for the domain with Access Manager 11.1.2 as follows:

1. Stopping Administration Server
2. Starting Administration Server

### Stopping Administration Server

To stop the Administration Server, do the following:

**On UNIX**:

1. Move from the present working directory to the directory `*MW_HOME*/user_projects/domains/*domain_name*/bin` using the command:

   ```
   cd MW_HOME/user_projects/domains/domain_name/bin/
   ```

2. Run the following command:

   ```
   ./stopWebLogic.sh admin_username admin_password admin_url
   ```

   In this command,

   *`admin_username`* is the username of the WebLogic Administration Server.

   *`admin_password`* is the password of the WebLogic Administration Server.

   *`admin_url`* is the URL of the administration console. It must be specified in the format `http://*host*:*port*/console`.

**On Windows**:

1. Move from your present working directory to the directory `*MW_HOME*\user_projects\domains\*domain_name*\bin` using the following command on the command line:

   ```
   cd MW_HOME\user_projects\domains\domain_name\bin\
   ```

2. Run the following command:

```
stopWebLogic.cmd
```

When prompted, enter the Administration Server username and password.

### Starting Administration Server

To start the WebLogic Administration Server, do the following:

**On UNIX**:

1. Move from your present working directory to the directory *MW_HOME*/user_projects/domains/*domain_name*/bin using the command:

   ```
   cd MW_HOME/user_projects/domains/domain_name/bin/
   ```

2. Run the following command:

   ```
   ./startWebLogic.sh
   ```

   When prompted, enter the WebLogic Administration Server username and password.

**On Windows**:

1. Move from your present working directory to the directory *MW_HOME*\user_projects\domains\*domain_name*\bin using the following command on the command line:

   ```
   cd MW_HOME\user_projects\domains\domain_name\bin\
   ```

2. Run the following command:

   ```
   startWebLogic.cmd
   ```

   When prompted, enter the WebLogic Administration Server username and password.

## 12.12 Additional Steps for Incremental Migration

Complete the following steps only if you wish to perform incremental migration:

1. Set the property `migration_mode` to `INCREMENTAL` in the properties file (Section 12.9, "Creating a Properties File") that you create during the migration process.

2. When you generate the assessment report (as described in Generating the Assessment Report), an input file called `IncludeFile.txt` is generated at the same location where the assessment report is generated. This text file contains agents and application domains of Oracle Access Manager 10*g* deployment. The agents and application domains are listed in the `IncludeFile.txt` as shown in the following example:

   ```
   AGENT##ag_one_12752##ag_one_12752##N
   AGENT##temp##temp##N
   APPLICATION_DOMAIN##20120304T01055680323##my_domain##N
   APPLICATION_DOMAIN##20120306T03491413638##Finance##N
   APPLICATION_DOMAIN##20120306T04155393859##HR##N
   APPLICATION_DOMAIN##20120319T0255014722##Domain With Resources Only##N
   APPLICATION_DOMAIN##20120319T03241993733##Domain with Policy##N
   APPLICATION_DOMAIN##20120319T03300047441##Domain with policy and authn rule##N
   APPLICATION_DOMAIN##20120319T03324669347##domain with policy and authz rule##N
   ```

To perform incremental migration, you must specify either a list of artifacts (agents and application domains) that you wish to migrate, or a list of artifacts (agents and application domains) that you wish to exclude from the migration. Therefore, you must create one of the following files:

- **include file**: This is a text file that contains the list of agents and application domains that you wish to migrate. You can either use the auto-generated `IncludeFile.txt` as the `include` file by marking the agents and application domains that you wish to migrate as `Y`, or manually create a new `include` file. However, it is recommended that you use the `IncludeFile.txt` to create the `include` file.

  To create the `include` file using the `IncludeFile.txt`, do the following:

  a. Copy the `IncludeFile.txt` to any accessible location, and rename it to `include.txt`, if required.

  b. Mark the agents and application domains that you wish to migrate as `Y`. `Y` indicates that the artifact is selected for incremental migration.

  c. Set the property `include_file` in the properties file (`oam_migration.properties`) to the absolute path to the `include` file.

  **Note:** If you wish to manually create the `include` file, specify the agents and application domains that you wish to migrate in the format specified in the following example:

  ```
  AGENT##temp##temp##Y

  APPLICATION_DOMAIN##20120304T01055680323##my_domain##Y
  ```

- **exclude file**: This is a text file that contains the list of agents and application domains that you wish to exclude from migration. You can either use the auto-generated `IncludeFile.txt` as the `exclude` file by marking the agents and application domains that you wish to exclude from migration as `Y`, or manually create a new `exclude` file. However, it is recommended that you use the `IncludeFile.txt` to create the `exclude` file.

  To create the `exclude` file using the `IncludeFile.txt`, do the following:

  a. Copy the `IncludeFile.txt` to any accessible location, and rename it to `exclude.txt`, if required.

  b. Mark the agents and application domains that you wish to exclude from migration as `Y`. `Y` indicates that the artifact is not selected for incremental migration.

  c. Set the property `exclude_file` in the properties file (`oam_migration.properties`) to the absolute path to the `exclude` file.

  **Note:** If you wish to manually create the `exclude` file, specify the agents and application domains that you wish to exclude from the incremental migration in the format specified in the following example:

  ```
  AGENT##temp##temp##Y

  APPLICATION_DOMAIN##20120304T01055680323##my_domain##Y
  ```

---

**Note:** If you create both the `include` file and the `exclude` file, and specify paths to both the files in the properties file, then the `include` file takes precedence, and the `exclude` file will be ignored.

If you do not specify any of these input files in the properties file, the migration will be aborted.

You can perform incremental migration more than once.

---

## 12.13 Migrating the Artifacts of Oracle Access Manager 10*g* to Access Manager 11.1.2

Before you migrate Oracle Access Manager 10*g* to Access Manager 11.1.2, it is recommended that you generate an assessment report (as described in Section 15.9, "Generating the Assessment Report"), and analyze what artifacts are compatible and incompatible in Access Manager 11.1.2.

---

**Note:** If you decide to migrate Oracle Access Manager 10*g* to Access Manager 11.1.2 after analyzing the assessment report, perform the steps 1 to 6 described in this section.

If you wish to perform incremental migration, make sure that you have set the property `migration_mode` to `INCREMENTAL` in the properties file. Also, ensure that you have completed the additional steps described in Section 12.12, "Additional Steps for Incremental Migration" before you follow the steps described in this section.

If you wish to perform complete migration, make sure that you have set the property `migration_mode` to `COMPLETE` in the properties file.

---

Complete the following steps to perform complete migration or incremental migration:

1. Set the value of `evaluate_only` property to `false` in the properties file that you created in Creating a Properties File. Save the file and close.
2. Run the following command to launch the WebLogic Scripting Tool (WLST):

   **On UNIX**:

   a. Move from your present working directory to the *`IAM_HOME`*`/common/bin` directory by running the following command on the command line:

   ```
   cd IAM_HOME/common/bin
   ```

   b. Run the following command to launch the WebLogic Scripting Tool (WLST):

   ```
   ./wlst.sh
   ```

   **On Windows**:

   a. Move from your present working directory to the *`IAM_HOME`*`\common\bin` directory by running the following command on the command line:

   ```
   cd IAM_HOME\common\bin
   ```

   b. Run the following command to launch the WebLogic Scripting Tool (WLST):

   ```
   wlst.cmd
   ```

3. Run the following command to connect WLST to the WebLogic Server instance:

```
connect('wls_admin_username','wls_admin_password','t3://hostname:port');
```

In this command,

*wls_admin_username* is the username of the WebLogic Administration Server.

*wls_admin_password* is the password of the WebLogic Administration Server.

*hostname* is the host on which WebLogic Administration Server is running.

*port* is the port of the WebLogic Administration Server.

For example:

```
connect('weblogic','password','t3://localhost:7001');
```

4. Run the following command:

```
domainRuntime();
```

5. Run the following command:

```
setLogLevel(logger="oracle.oam",level="TRACE:32",persist="0",target="AdminServe
r");
```

6. Run the following command to migrate the artifacts of Oracle Access Manager 10*g* to Access Manager 11.1.2:

```
oamMigrate(oamMigrateType="OAM10g",pathMigrationPropertiesFile="absolute_path_
of_properties_file");
```

where

*absolute_path_of_properties_file* is the absolute path of the properties file that you created in Creating a Properties File. For example:

**On UNIX**:
`oamMigrate(oamMigrateType="OAM10g",pathMigrationPropertiesFile="abc/def/oam_migration.properties"`

**On Windows**:
`oamMigrate(oamMigrateType="OAM10g",pathMigrationPropertiesFile="abc\\def\\oam_migration.properties"`

When the migration is complete, the WLST console displays a message that indicates the result of the migration. The log files are generated at the following location:

**On UNIX**: `MW_HOME/user_projects/domains/base_domain/servers/AdminServer/logs/Adminserver-diagnostic*.log`

**On Windows**: `MW_HOME\user_projects\domains/base_domain\servers\AdminServer\logs/Adminserver-diagnostic*.log`

In case of any errors during the migration process, refer to the log files.

## 12.14 Configuring Centralized Logout for 10*g* WebGates with Access Manager 11.1.2

If you are using 10*g* WebGates with Access Manager 11.1.2, you must configure the centralized logout settings for 10*g* WebGates to work with Access Manager 11.1.2 server, after migrating Oracle Access Manager 10*g* to Access Manager 11.1.2.

For more information about configuring centralized logout for 10*g* WebGates, see "Configuring Centralized Logout for 10g Webgate with 11g OAM Servers" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.

> **Note:** Skip this step if you are not using 10*g* WebGates with Access Manager 11.1.2.

## 12.15 Associating the WebGates with Access Manager 11.1.2 Server

After you migrate Oracle Access Manager 10*g* to Access Manager 11.1.2, you must associate all of the migrated WebGates with the Access Manager 11.1.2 Server. To do this, complete the following steps:

1. Create a new server profile on Oracle Access Manager 10*g* Access System console with the hostname and port details of the Access Manager 11.1.2 Server instance, by doing the following:

   a. Log in to the Oracle Access Manager 10*g* Access System console.

   b. Go to the **Access System Configuration** tab.

   c. Click **Access Server Configuration** on the left navigation pane.

   d. Click **Add** to create a new server profile.

   e. Specify the following details:

      **Name**: Specify a name for this server.

      **Hostname**: Specify the hostname of the machine on which Access Manager 11.1.2 Server instance is running.

      **Port**: Specify the proxy port for Access Manager 11.1.2 Server instance. The default proxy port for Access Manager 11.1.2 is `5575`.

      **Transport Security**: Specify the same transport security mode as that of the Access Manager 11.1.2 Server instance.

      Keep the default values for other parameters.

   f. Click **Save**.

2. Set the value of `MAX Connections` parameter of the WebGate (AccessGate) in the WebGate profile such that the WebGate does not establish connection with the Access Manager 11.1.2 Server after association.

   If all of the Oracle Access Manager 10*g* primary servers are up, set the value of `MAX Connections` equal to the sum of the number of connections to all the primary Oracle Access Manager 10*g* servers.

   For more information about modifying a WebGate profile, see "Modifying an AccessGate" in the *Oracle Access Manager Access Administration Guide* for release 10*g* (10.1.4.3).

3. Associate each of the WebGates with the Access Manager 11.1.2 Server as one or more primary servers, by retaining the existing Oracle Access Manager 10*g* server. Set the number of connections to the Access Manager 11.1.2 server as 1 or more.

   After the inactive reconfiguration period, the WebGate is updated with the new list of servers.

4. Optional: For each WebGate, make sure that the file `ObAccessClient.xml` at the location *`webgate_installation_directory`*`/oblix/lib/ObAccessClient.xml` is

updated with the host and port of the Access Manager 11.1.2 Server in the list of primary servers. To do this, open the `ObAccessClient.xml` file and look for the list of primary servers.

5. Point the WebGate to the Access Manager 11.1.2 server by performing one of the following tasks:

   - Stop all the Oracle Access Manager 10*g* Servers. If the number of connections to Oracle Access Manager 10*g* servers is high, WebGate takes a few minutes to start talking to the Access Manager 11.1.2 Server. If you restart the web server that hosts the WebGate, WebGate starts talking to the Access Manager 11.1.2 server immediately.

   - Increase the value of the parameter `MAX Connections` by one, so that the WebGate establishes the connection with Access Manager 11.1.2 server. If the load on WebGate is more, it takes less time to connect to the Access Manager 11.1.2 Server.

   WebGate now gets the new configuration information from the Access Manager 11.1.2 Server, which has only one primary server. Thus, the WebGate communicates only with the Access Manager 11.1.2 server. Once this is done, you can reduce the value of `MAX Connections` as there is only one server.

## 12.16 Verifying the Migration

To verify the migration, do the following:

1. The message "Migration completed successfully" is displayed on the WLST console if the migration is successful.

2. Verify the migration details like upgraded status, type of migration, timestamp and so on, in the `oam-config.xml` file that is generated in the following directory:

   **On UNIX**:

   ```
   MW_HOME/user_projects/domains/Domain_Name/config/fmwconfig/
   ```

   **On Windows**:

   ```
   MW_HOME\user_projects\domains\Domain_Name\config\fmwconfig\
   ```

3. Log in to the Oracle Access Management console using the following URL:

   ```
   http://host:port/oamconsole
   ```

   In this URL, *host* is the machine on which Access Manager 11.1.2 is running, and *port* is the port number.

   Verify that the Oracle Access Manager 10*g* artifacts are migrated to Access Manager 11.1.2.

## 12.17 Troubleshooting

This section describes solutions to the common problems that you might encounter when migration Oracle Access Manager 10*g* to Access Manager 11.1.2. It contains the following topics:

- Increasing the Size of the Log File to Avoid the Loss of Migration Data
- Increasing the Heap Size of the WebLogic Server

### 12.17.1 Increasing the Size of the Log File to Avoid the Loss of Migration Data

If the size of the log file is too small, the migration data might get lost when the logs files are rotated. To overcome this, you must increase the size of the log file in the WebLogic console by doing the following:

1. Log in to the WebLogic Administration console using the following URL:

   ```
   http://host:port/console
   ```

   In this URL, *host* is the hostname of the machine hosting WebLogic Administration Server, and *port* is the port number of the Administration Server.

2. Under **Domain Structure** on the left navigation pane, expand **Environment** under the respective domain name.
3. Click **Servers**.
4. On the **Summary of Servers** page, go to the **Configuration** tab, and click on the name of the Administration Server (For example, **AdminServer(admin)**).
5. Go to the **Logging** tab, and click the **General** tab.
6. Specify the right values for the following fields:

   a. **Rotation file size**: Specify the size of the log file in KiloBytes. The maximum value that can be specified is 65535 KB.

   b. **Files to retain**: Specify the number of rotated log files you wish to retain.

7. Click **Save**.

### 12.17.2 Increasing the Heap Size of the WebLogic Server

If the Oracle Access Manager 10*g* policy data is large in terms of number of various policy related artifacts, the migration tool may need large memory for processing. If the WebLogic Administration Server has small heap size, you can increase it by doing the following:

**On UNIX**:

1. Open the `setDomainEnv.sh` file in any text editor, from the directory *`MW_HOME`*`/user_projects/domains/`*`Domain_Name`*`/bin/`.
2. Search for the following line:

   ```
   if [ "${USER_MEM_ARGS}" != "" ]
   ```

3. Add the following lines just before the line identified in the previous step.

   ```
   USER_MEM_ARGS="new_heap_size"
   export USER_MEM_ARGS
   ```

   where, *`new_heap_size`* is the new heap size of the WebLogic Administration Server in MegaBytes.

   For example, if you wish to increase the heap size of the WebLogic Administration Server to 2GB, specify as shown below:

   ```
   USER_MEM_ARGS="-Xms2048m -Xmx2048m"
   export USER_MEM_ARGS
   ```

**On Windows**:

1. Open the `setDomainEnv.cmd` file in any text editor, from the directory *`MW_HOME`*`\user_projects\domains\`*`Domain_Name`*`\bin\`.

2. Search for the following line:

   ```
   if NOT "%USER_MEM_ARGS%"=="" (
   ```

3. Add the following line just before the line identified in the previous step.

   ```
   set USER_MEM_ARGS="new_heap_size"
   ```

   where, *new_heap_size* is the new heap size of the WebLogic Administration Server in MegaBytes.

   For example, if you wish to increase the heap size of the WebLogic Administration Server to 2GB, specify as shown below:

   ```
   set USER_MEM_ARGS=-Xms2048m -Xmx2048m
   ```

# 13 Migrating Oracle Adaptive Access Manager 10*g* Environments

This chapter describes how to migrate Oracle Adaptive Access Manager (OAAM) 10*g* to Oracle Adaptive Access Manager 11*g* Release 2 (11.1.2). The chapter contains the following sections:

## 13.1 Migration Overview

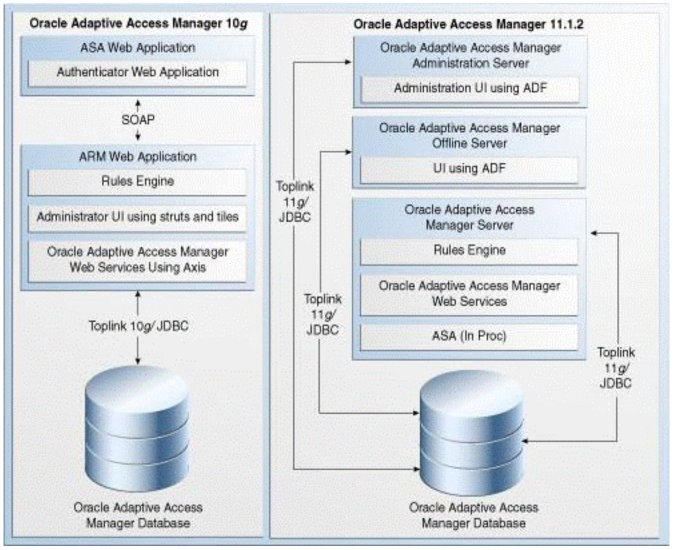
The process for migrating OAAM 10*g* to OAAM 11.1.2 involves installing Oracle Identity and Access Management 11*g* Release 2 (11.1.2), configuring OAAM 11.1.2, upgrading OAAM 10*g* schemas, configuring the database security store, and upgrading the Oracle Adaptive Access Manager middle tier.

For more information about other migration scenarios, see Section 1.3, "Migration and Coexistence Scenarios".

## 13.2 Topology Comparison

Figure 13–1 compares the topologies of OAAM 10*g* and OAAM 11.1.2.

*Figure 13–1 Comparison of OAAM 10g and OAAM 11g Topologies*


Oracle Adaptive Access Manager 10g
ASA Web Application
Authenticator Web Application
SOAP
ARM Web Application
Rules Engine
Administrator UI using struts and tiles
Oracle Adaptive Access Manager Web Services Using Axis
Toplink 10g/JDBC
Oracle Adaptive Access Manager Database
Oracle Adaptive Access Manager 11.1.2
Oracle Adaptive Access Manager Administration Server
Administration UI using ADF
Oracle Adaptive Access Manager Offline Server
UI using ADF
Oracle Adaptive Access Manager Server
Rules Engine
Oracle Adaptive Access Manager Web Services
ASA (In Proc)
Toplink 11g/ JDBC
Toplink 11g/ JDBC
Toplink 11g/ JDBC
Oracle Adaptive Access Manager Database

## 13.3 Migration Roadmap

Table 13–1 provides the migration roadmap.

*Table 13–1 Task Roadmap*

| Task No | Task | For More Information |
|---|---|---|
| 1 | Complete the prerequisites. | See, Prerequisites for Migration |
| 2 | Install Oracle Identity and Access Management 11.1.2. | See, Installing Oracle Identity and Access Management 11.1.2 |
| 3 | Create Oracle Platform Security Services (OPSS) schema, and Metadata Services (MDS) schema using Repository Creation Utility (RCU). | See, Creating Oracle Platform Security Services Schema |
| 4 | Upgrading the OAAM schema. | See, Upgrading OAAM 10g Schema |
| 5 | Configure OAAM 11.1.2 in a new or existing domain. | See, Configuring OAAM 11.1.2 in a New or Existing Oracle WebLogic Domain |
| 6 | Configure the database security store by running the `configuresecuritystore.py` script. | See, Configuring Database Security Store |
| 7 | Configure the Node Manager. | See, Configuring Node Manager |
| 8 | Start the WebLogic Administration Server. | See, Starting the WebLogic Administration Server |

*Table 13–1 (Cont.) Task Roadmap*

| Task No | Task | For More Information |
|---|---|---|
| 9 | Stop the OAAM Managed Servers (OAAM Admin Server, OAAM Server, and OAAM Offline Server). | See, Stopping OAAM Managed Servers |
| 10 | Upgrade the OAAM middle tier using Upgrade Assistant. | See, Upgrading OAAM Middle Tier Using Upgrade Assistant |
| 11 | Start the OAAM Managed Servers (OAAM Admin Server, OAAM Server, and OAAM Offline Server). | See, Starting OAAM Managed Servers |
| 12 | Verify the migration. | See, Verifying the Migration |

## 13.4 Prerequisites for Migration

You must complete the following prerequisites for migrating Oracle Adaptive Access Manager 10*g* to Oracle Adaptive Access Manager 11.1.2:

1. Read the Oracle Fusion Middleware System Requirements and Specifications document to ensure that your environment meets the minimum requirements for the products you are installing, upgrading, and migrating.

   **Note:** For information about Oracle Fusion Middleware concepts and directory structure, see "Understanding Oracle Fusion Middleware Concepts and Directory Structure" in the *Oracle Fusion Middleware Installation Planning Guide for Oracle Identity and Access Management*.

2. Verify that the Oracle Adaptive Access Manager 10*g* version that you are using is supported for migration. For information about supported starting points for Oracle Adaptive Access Manager 10*g* migration, see Section 11.3, "Supported Starting Points for Oracle Adaptive Access Manager 10g Migration".

## 13.5 Installing Oracle Identity and Access Management 11.1.2

As part of the migration process, you must install Oracle Identity and Access Management 11*g* Release 2 (11.1.2).

For information about installing Oracle Identity and Access Management 11.1.2, see "Installing Oracle Identity and Access Management (11.1.2)" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

## 13.6 Creating Oracle Platform Security Services Schema

Create the following schemas by running the Repository Creation utility (RCU) 11.1.2. IAU (Audit Schema) is optional.

- **Oracle Platform Security Services** (OPSS) - (mandatory)
- **Metadata Services** (MDS) - (mandatory)

- **IAU** (Audit Schema) - (optional)

For more information about creating schemas, see "Creating Schemas" in the *Using Repository Creation Utility*.

## 13.7 Upgrading OAAM 10*g* Schema

You must upgrade the OAAM 10*g* schema to 11.1.2 using a WLST command. To do this, complete the following steps:

1. You must update the `access_upgrade.properties` file available at the following location with the right database connection details:

   **On UNIX**: `MW_HOME/IAM_HOME/common/wlst/access_upgrade.properties`

   **On Windows**: `MW_HOME\IAM_HOME\common\wlst\access_upgrade.properties`

   In the `access_upgrade.properties` file, specify the right values for the following properties:

   - `OAAM_DB_SCHEMA_USERNAME=OAAM_Database_schema_username`
   - `OAAM_DB_URL=OAAM_Database_URL`
   - `OAAM_DB_SYS_USERNAME=OAAM_DB_sys_username`
   - `OAAM_DB_10g=true`

   where

   *`OAAM_Database_schema_username`* is the username of the OAAM database schema

   *`OAAM_Database_URL`* is the URL of the database where schemas are used. It must be specified in the format *`hostname`*:*`port`*:*`sid`*.

   *`OAAM_DB_sys_username`* is the username of the database system administrator

   You must set the value of the property `OAAM_DB_10g` to `true,` as you are upgrading OAAM 10*g*

2. Run the following command to launch the WebLogic Scripting Tool (WLST):

   **On UNIX**:

   a. Move from your present working directory to the `IAM_HOME/common/bin` directory by running the following command on the command line:

   ```
   cd IAM_HOME/common/bin
   ```

   b. Run the following command to launch the WebLogic Scripting Tool (WLST):

   ```
   ./wlst.sh
   ```

   **On Windows**:

   a. Move from your present working directory to the `IAM_HOME\common\bin` directory by running the following command on the command line:

   ```
   cd IAM_HOME\common\bin
   ```

   b. Run the following command to launch the WebLogic Scripting Tool (WLST):

   ```
   wlst.cmd
   ```

3. Run the following WLST command offline, to upgrade the OAAM 10*g* schema to 11.1.2:

   **On UNIX**:

```
upgradeAccessSchema(filePath="MW_HOME/IAM_HOME/common/wlst/access_
upgrade.properties")
```

**On Windows**:

```
upgradeAccessSchema(filePath="MW_HOME\\IAM_HOME\\common\\wlst\\access_
upgrade.properties")
```

## 13.8 Configuring OAAM 11.1.2 in a New or Existing Oracle WebLogic Domain

After you install the software, you must configure Oracle Adaptive Access Manager 11.1.2. You can configure OAAM either in a new or in an existing domain. For more information, see "Configuring Oracle Adaptive Access Manager" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

> **Note:** Ensure that you specify the Oracle Adaptive Access Manager 10*g* database details in the screen where it prompts you to enter the Oracle Adaptive Access Manager 11*g* database details. You must enter the 10*g* credentials because there is no separate 11*g* database. It checks the database for a few system tables, which are not present in Oracle Adaptive Access Manager 10*g* database.

## 13.9 Configuring Database Security Store

After you configure OAAM 11.1.2 in a domain, you must run the `configuresecuritystore.py` script to configure the Database Security Store. For more information, see "Configuring Database Security Store for an Oracle Identity and Access Management Domain" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

> **Note:** If you have already run the `configuresecuritystore.py` script as part of the OAAM 11.1.2 configuration in Section 13.8, ignore this task.

## 13.10 Configuring Node Manager

If you wish to start and stop the Managed Servers through the WebLogic Administration console, you must configure the Node Manager, and start it. For information about configuring Node Manager, see "Configuring Node Manager to Start Managed Servers" in the *Oracle Fusion Middleware Administrator's Guide*.

## 13.11 Starting the WebLogic Administration Server

You must start the WebLogic Administration Server, do the following:

**On UNIX**:

1. Move from your present working directory to the `MW_HOME/user_projects/domains/domain_name/bin` directory using the command:

   ```
   cd MW_HOME/user_projects/domains/domain_name/bin/
   ```

2. Run the following command:

```
./startWebLogic.sh
```

When prompted, enter the WebLogic Administration Server username and password.

**On Windows**:

1. Move from your present working directory to the *MW_HOME*\user_projects\domains\*domain_name*\bin directory using the following command on the command line:

   ```
   cd MW_HOME\user_projects\domains\domain_name\bin\
   ```

2. Run the following command:

   ```
   startWebLogic.cmd
   ```

   When prompted, enter the WebLogic Administration Server username and password.

## 13.12 Stopping OAAM Managed Servers

If you have started the OAAM Admin Server, OAAM Offline Server (if present), and OAAM Server, you must stop all of them before you can upgrade the OAAM middle tier in section 13.10. To stop these servers, do the following:

**On UNIX**:

1. Move from your present working directory to the directory *MW_HOME*/user_projects/domains/*domain_name*/bin directory using the command:

   ```
   cd MW_HOME/user_projects/domains/domain_name/bin/
   ```

2. Run the following command to stop the OAAM Admin Server:

   ```
   ./stopManagedWebLogic.sh oaam_admin_server admin_url username password
   ```

   In this command,

   *oaam_admin_server* is the name of the OAAM Admin Server.

   *admin_url* is the URL of the WebLogic Administration console. Specify this parameter only if the WebLogic Administration Server is on a different machine. You must specify the URL in the format http://*host*:*port*/console.

   *username* is the username of WebLogic Administration Server.

   *password* is the password of WebLogic Administration Server.

3. Run the following command to stop the OAAM Offline Server:

   ```
   ./stopManagedWebLogic.sh oaam_offline_server admin_url username password
   ```

   In this command,

   *oaam_offline_server* is the name of the OAAM Offline Server.

   *admin_url* is the URL of the WebLogic Administration console. Specify this parameter only if the WebLogic Administration Server is on a different machine. You must specify the URL in the format http://*host*:*port*/console.

   *username* is the username of WebLogic Administration Server.

   *password* is the password of WebLogic Administration Server.

4. Run the following command to stop the OAAM Server:

   ```
   ./stopManagedWebLogic.sh oaam_server admin_url username password
   ```

   In this command,

   *oaam_server* is the name of the OAAM Server.

   *admin_url* is the URL of the WebLogic Administration console. Specify this parameter only if the WebLogic Administration Server is on a different machine. You must specify the URL in the format `http://host:port/console`.

   *username* is the username of WebLogic Administration Server.

   *password* is the password of WebLogic Administration Server.

**On Windows**:

1. Move from the present working directory to the `MW_HOME\user_projects\domains\domain_name\bin` directory using the following command on the command line:

   ```
   cd MW_HOME\user_projects\domains\domain_name\bin\
   ```

2. Run the following command to stop the OAAM Admin Server:

   ```
   stopManagedWebLogic.cmd oaam_admin_server admin_url username password
   ```

   In this command,

   *oaam_admin_server* is the name of the OAAM Admin Server

   *admin_url* is the WebLogic Administration console. Specify this parameter only if the WebLogic Administration Server is on a different machine. You must specify the URL in the format `http://host:port/console`.

   *username* is the username of WebLogic Administration Server.

   *password* is the password of WebLogic Administration Server.

3. Run the following command to stop the OAAM Offline Server:

   ```
   stopManagedWebLogic.cmd oaam_offline_server admin_url username password
   ```

   In this command,

   *oaam_offline_server* is the name of the OAAM Offline Server.

   *admin_url* is the URL of the WebLogic Administration console. Specify this parameter only if the WebLogic Administration Server is on a different machine. You must specify the URL in the format `http://host:port/console`.

   *username* is the username of WebLogic Administration Server.

   *password* is the password of WebLogic Administration Server.

4. Run the following command to stop the OAAM Server:

   ```
   stopManagedWebLogic.cmd oaam_server admin_url username password
   ```

   In this command,

   *oaam_server* is the name of the OAAM Server.

   *admin_url* is the URL of the WebLogic Administration console. Specify this parameter only if the WebLogic Administration Server is on a different machine. You must specify the URL in the format `http://host:port/console`.

*username* is the username of WebLogic Administration Server.

*password* is the password of WebLogic Administration Server.

> **Note:** If you have more than one OAAM Server, you must stop all of them.

## 13.13 Upgrading OAAM Middle Tier Using Upgrade Assistant

You must upgrade the OAAM 10*g* middle tier using Upgrade Assistant. To do this, complete the following steps:

1. If you have started the Oracle Adaptive Access Manager Managed Servers, they auto-generate symmetric keys required for encryption or decryption. You must delete the keys before performing middle tier upgrade. To do so, complete the following steps:

   a. Log in to Oracle Enterprise Manager using the URL:

   ```
   host:port/em
   ```

   b. Expand the WebLogic Domain on the left pane, and select the **OAAM** domain.

   The OAAM domain page is displayed.

   c. From the OAAM Domain, select **Security**, and then **Credentials**.

   The **Credentials** page is displayed.

   d. Expand **oaam** and delete the entries related to symmetric keys.

2. Launch Upgrade Assistant by doing the following:

   **On UNIX**:

   a. Move from your present working directory to the `MW_HOME/IAM_HOME/bin` directory using the following command:

   ```
   cd MW_HOME/IAM_HOME/bin
   ```

   b. Run the following command:

   ```
   ./ua
   ```

   **On Windows**:

   a. Move from your present working directory to the `MW_HOME\IAM_HOME\bin` directory using the following command on the command line:

   ```
   cd MW_HOME\IAM_HOME\bin
   ```

   b. Run the following command:

   ```
   ua.bat
   ```

   The Oracle Fusion Middleware Upgrade Assistant **Welcome** screen is displayed.

3. Click **Next**.

   The **Specify Operation** screen is displayed.

4. Select **Upgrade Oracle Adaptive Access Manager Middle Tier**.

   The options available in Upgrade Assistant are specific to the Oracle home from which it started. When you start Upgrade Assistant from an Oracle Application

Server Identity Management Oracle home, the options shown on the Specify Operation screen are the valid options for an Oracle Application Server Identity Management Oracle home.

5. Click **Next**.

   The **Specify Source Details** screen is displayed.

6. Enter the following information:

   - Click **Browse** and enter the directory location for Oracle Adaptive Access Manager Adaptive Strong Authenticator Web Application 10*g* (ASA) and Adaptive Risk Manager Web Application 10*g* (ARM) applications.
   - **Database Type**: Select the database type from the drop-down list.
   - **Connect String**: Enter the name of the server where your database is running. Use one of the following formats for Oracle Database:

     `//`*`host`*`:`*`port`*`/service` or *`host`*`:`*`port`*`:`*`sid`*

   - **Schema User Name**: Enter the user name for the OAAM schema.
   - **Schema Password**: Enter the password for the OAAM schema.

7. Click **Next**.

   The **Specify WebLogic Server** screen is displayed.

8. Enter the following information about your Oracle WebLogic Server domain:

   - **Host**: The host name of the machine where WebLogic Administration Server is running.
   - **Port**: The listening port of the Administration Server. The default Administration Server port is `7001`.
   - **Username**: The user name that is used to log in to the Administration Server. This is the same username you use to log in to the Administration Console for the domain.
   - **Password**: The password for the administrator account that is used to log in to the Administration Server. This is the same password you use to log in to the Administration Console for the domain.
   - Click **Next**.

   The **Specify Upgrade Options** screen is displayed.

9. Select **Start destination components after successful upgrade**, and click **Next**.

   The **Examining Components** screen is displayed.

   **Note:** Ensure that Node Manager is running, before you select **Start destination components after successful upgrade**.

10. Click **Next**.

    The **Upgrade Summary** screen is displayed.

11. Click **Upgrade**.

    The **Upgrade Progress** screen is displayed. This screen provides the following information:

    - The status of the upgrade

- Any errors or problems that occur during the upgrade

12. Click **Next**.

    The **Upgrade Complete** screen is displayed. This screen confirms that the upgrade was complete.

13. Click **Close**.

## 13.14 Starting OAAM Managed Servers

You must start the OAAM Managed Servers in the following order:

1. OAAM Admin Server
2. OAAM Offline Server, if you have configured OAAM Offline Server
3. OAAM Server

To start these servers, do the following:

**On UNIX**:

1. Move from your present working directory to the *MW_HOME*/user_projects/domains/*domain_name*/bin directory using the command:

   ```
   cd MW_HOME/user_projects/domains/domain_name/bin/
   ```

2. Run the following command to start the OAAM Admin Server:

   ```
   ./startManagedWebLogic.sh oaam_admin_server admin_url
   ```

   In this command,

   *oaam_admin_server* is the name of the OAAM Admin Server.

   *admin_url* is the URL of the WebLogic Administration console. Specify this parameter only if the WebLogic Administration Server is on a different machine. You must specify the URL in the format `http://`*host*`:`*port*`/console`.

   When prompted, enter the username and password of the WebLogic Administration Server.

3. Run the following command to start the OAAM OfflineServer:

   ```
   ./startManagedWebLogic.sh oaam_offline_server admin_url
   ```

   In this command,

   *oaam_offline_server* is the name of the OAAM Offline Server.

   *admin_url* is the URL of the WebLogic Administration console. Specify this parameter only if the WebLogic Administration Server is on a different machine. You must specify the URL in the format `http://`*host*`:`*port*`/console`.

   When prompted, enter the username and password of the WebLogic Administration Server.

4. Run the following command to start the OAAM Server:

   ```
   ./startManagedWebLogic.sh oaam_server admin_url
   ```

   In this command,

   *oaam_server* is the name of the OAAM Server *admin_url* is the URL of the WebLogic Administration console. Specify this parameter only if the WebLogic Administration Server is on a different machine. You must specify the URL in the format `http://`*host*`:`*port*`/console`.

When prompted, enter the username and password of the WebLogic Administration Server.

**On Windows**:

1. Move from the present working directory to the *MW_HOME*`\user_projects\domains\`*domain_name*`\bin` directory using the command:

   ```
   cd MW_HOME\user_projects\domains\domain_name\bin\
   ```

2. Run the following command to start the OAAM Admin Server:

   ```
   startManagedWebLogic.cmd oaam_admin_server admin_url
   ```

   In this command,

   *oaam_admin_server* is the name of the OAAM Admin Server.

   *admin_url* is the URL of the WebLogic Administration console. Specify this parameter only if the WebLogic Administration Server is on a different machine. You must specify the URL in the format `http://`*host*`:`*port*`/console`.

   When prompted, enter the username and password of the WebLogic Administration Server.

3. Run the following command to start the OAAM Offline Server:

   ```
   startManagedWebLogic.cmd oaam_offline_server admin_url
   ```

   In this command,

   *oaam_offline_server* is the name of the OAAM Offline Server.

   *admin_url* is the URL of the WebLogic Administration console. Specify this parameter only if the WebLogic Administration Server is on a different machine. You must specify the URL in the format `http://`*host*`:`*port*`/console`.

   When prompted, enter the username and password of the WebLogic Administration Server.

4. Run the following command to start the OAAM Server:

   ```
   startManagedWebLogic.cmd oaam_server admin_url
   ```

   In this command,

   *oaam_server* is the name of the OAAM Server.

   *admin_url* is the URL of the WebLogic Administration console. Specify this parameter only if the WebLogic Administration Server is on a different machine. You must specify the URL in the format `http://`*host*`:`*port*`/console`.

   When prompted, enter the username and password of the WebLogic Administration Server.

   > **Note:** Make sure that the OAAM Admin Server is running before you start the OAAM Server.

## 13.15 Verifying the Migration

To verify if the OAAM 10*g* migration was successful, do the following:

1. Log in to the administration console of Oracle Adaptive Access Manager 11.1.2, using the administration server username and password, and verify whether the OAAM 10*g* artifacts are migrated to OAAM 11*g*. Use the following URL to log in to the OAAM Admin Server:

   ```
   http://host:port/oaam_admin
   ```

   where

   `host` is the machine on which OAAM Admin Server is running

   `port` is the port number of the OAAM Admin Server

2. Create a user, and assign the `Investigator` role. Log in to the OAAM Admin Server with this user, and verify that you see the Investigator UI successfully.

   For more information about creating OAAM users, see "Creating OAAM Users" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*.

# 14 Migrating Oracle Single Sign-On 10*g* Environments

This chapter describes how to migrate your existing Oracle Single Sign-On 10*g* to Oracle Access Management Access Manager (Access Manager) 11*g* Release 2 (11.1.2).

This chapter contains the following sections:

## 14.1 Migration Overview

The process of migrating Oracle Single Sign-On 10*g* to Access Manager 11.1.2 involves installing Oracle Identity and Access Management 11.1.2, configuring Oracle Access Management Access Manager 11.1.2, and upgrading the Access Manager middle tier. Oracle Single Sign-On 10*g* to Access Manager 11.1.2 migration has three scenarios:

- Oracle Delegated Administration Services required after migrating Oracle Single Sign-On 10*g* to Access Manager 11.1.2
- Oracle Delegated Administration Services required, but Oracle Single Sign-On admin not required after migrating Oracle Single Sign-On 10*g* to Access Manager 11.1.2
- Oracle Delegated Administration Services not required after migrating Oracle Single Sign-On 10*g* to 11.1.2

Depending upon the scenario you choose, you must perform the corresponding tasks listed in Migration Roadmap.

For more information about other migration scenarios, see Section 1.3, "Migration and Coexistence Scenarios".

## 14.2 Migration Summary

You can use Oracle Fusion Middleware Upgrade Assistant to migrate the following:

- Oracle Single Sign-On 10*g* configurations and artifacts
- Partner metadata stored by Oracle Single Sign-On 10*g* Server
- Partners registered with Oracle Single Sign-On 10*g* Server

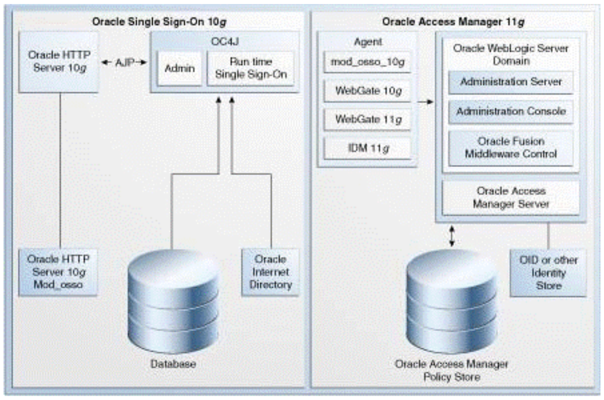
The following components are not migrated to Access Manager 11.1.2 environment when you run Upgrade Assistant to migrate from Oracle Single Sign-On 10*g*:

- Oracle Single Sign-On 10*g* with Window Native Authentication integration. For more information, see "Configuring Oracle Access Manager to use Windows Native Authentication" in the *Oracle Fusion Middleware Integration Guide for Oracle Access Manager*.
- Logging configuration. For more information see "Logging Component Event Messages" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.
- Oracle Single Sign-On 10*g* with Oracle Identity Federation integration. For more information, see "Integrating Oracle Identity Federation" in the *Oracle Fusion Middleware Integration Guide for Oracle Access Manager*.
- Custom authentication.
- X509 configurations. For more information, see *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.
- External Application.
- Policy stores.
- Multirealm configuration.

## 14.3 Topology Comparison

Figure 14–1 compares a typical Oracle Single Sign-On topology in Oracle Application Server 10*g* with an Access Manager 11.1.2 topology in Oracle Fusion Middleware 11*g*.

***Figure 14–1 Comparison of Typical Oracle Single Sign-On Topologies in Oracle Application Server 10g and Oracle Fusion Middleware 11g***


Oracle Single Sign-On 10*g*
Oracle HTTP Server 10*g*
AJP
OC4J
Admin
Run time Single Sign-On
Oracle HTTP Server 10*g* Mod_osso
Database
Oracle Internet Directory
Oracle Access Manager 11*g*
Agent
mod_osso_10*g*
WebGate 10*g*
WebGate 11*g*
IDM 11*g*
Oracle WebLogic Server Domain
Administration Server
Administration Console
Oracle Fusion Middleware Control
Oracle Access Manager Server
OID or other Identity Store
Oracle Access Manager Policy Store

## 14.4 Migration Scenarios

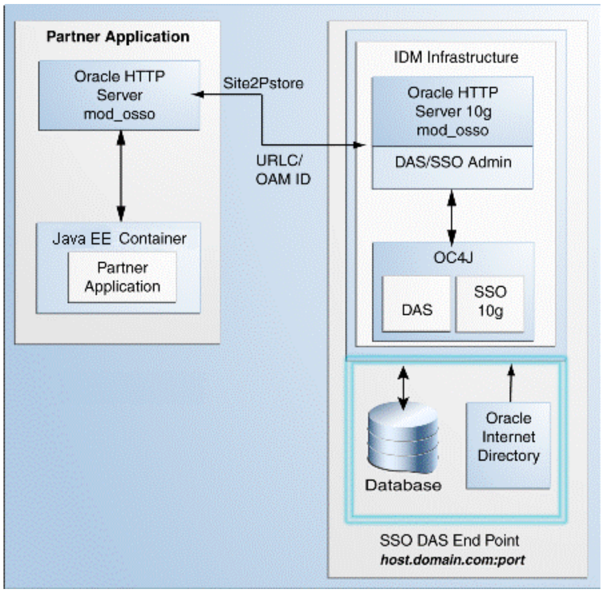
Before you migrate Oracle Single Sign-On 10*g* to Access Manager 11.1.2, you must consider your Oracle Single Sign-On 10*g* infrastructure (Figure 14–2) and depending on the functionality you choose to retain, you must select one of the following scenarios:

- Oracle Delegated Administration Services Required After Migrating Oracle Single Sign-On 10g to Access Manager 11.1.2
- Oracle Delegated Administration Services Required, but Oracle Single Sign-On Admin Not Required After Migrating Oracle Single Sign-On to Access Manager 11.1.2
- Oracle Delegated Administration Services Not Required After Migrating Oracle Single Sign-On to Access Manager 11.1.2

### Oracle Single Sign-On 10*g* Infrastructure Before Migration

Figure 14–2 illustrates the Oracle Single Sign-On 10*g* topology.

*Figure 14–2 Oracle Single Sign-On 10g Infrastructure*



The topology comprises the following:

- Partner applications in a Java EE container front-ended by Oracle HTTP Server to communicate with the Oracle Single Sign-On infrastructure
- Oracle Identity Management infrastructure that includes the Oracle HTTP Server 10*g* front-ending the Oracle Delegated Administration Services application and the Oracle Single Sign-On Server

The Oracle Single Sign-On endpoint, which consists of a host name and a port number, represents the URL that Oracle Single Sign-On users can use to access the Oracle Single Sign-On Server and the Oracle Delegated Administration Services application.

An example of Oracle Single Sign-On endpoint is `host.domain.com:port`.

**Note:** The example is used in this section to illustrate different migration scenarios and their Oracle Single Sign-On endpoints.

## 14.4.1 Oracle Delegated Administration Services Required After Migrating Oracle Single Sign-On 10*g* to Access Manager 11.1.2

Use this migration scenario if you want to continue to use the Oracle Delegated Administration Services (DAS) application and the Oracle Single Sign-On Admin tool after migrating from Oracle Single Sign-On 10*g* to Access Manager 11.1.2. Figure 14–3 illustrates the scenario.

Note the following points when using this migration scenario:

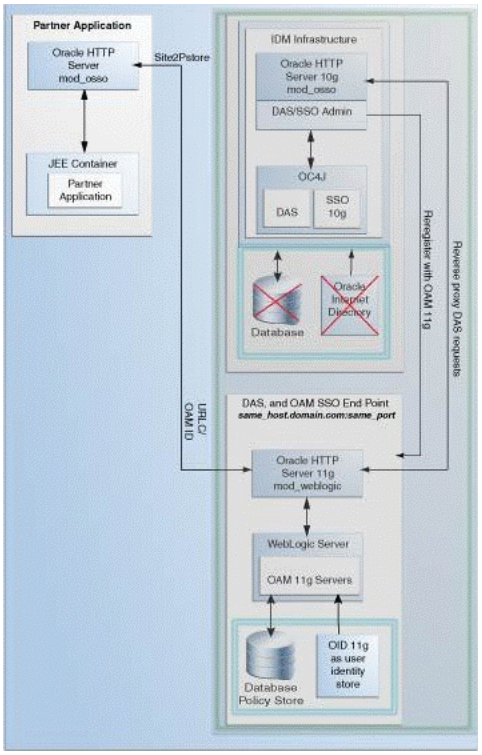
- Use this scenario if you are using Oracle Portal partner applications because you require Oracle Delegated Administration Services and Oracle Single Sign-On Administration. Migrate all partner applications at once.
- You are using the same Oracle HTTP Server 10*g* port that front-ended Oracle Single Sign-On 10*g* as the new port for Oracle Access Manager 11.1.2. Therefore, the Oracle Single Sign-On 10*g* server is no longer accessed. Instead, partner applications use Access Manager 11.1.2.

- The Oracle Delegated Administration Services (DAS) application runs on a new port.
- Any Oracle Delegated Administration Services requests from partner applications, such as Oracle Portal, arrive at the Oracle HTTP Server 11*g* and are redirected to Oracle HTTP Server 10*g*, which front-ends the Oracle Delegated Administration Services 10*g* application.

> **Note:** You must reregister Oracle Delegated Administration Services and Oracle Single Sign-On Admin with Oracle Access Manager 11.1.2 because their port is changed.

- The Oracle Single Sign-On-Oracle Delegated Administration Services endpoint (`same_host.domain.com:same_port`) remains the same for all the partner applications.
- After you perform the migration, Oracle Internet Directory is selected as the user identity store automatically.

***Figure 14–3 Oracle Delegated Administration Services Required After Migrating from Oracle Single Sign-On***


Partner Application
Oracle HTTP Server mod_osso
JEE Container
Partner Application
Site2Pstore
URLC/ OAM ID
IDM Infrastructure
Oracle HTTP Server 10g mod_osso
DAS/SSO Admin
OC4J
DAS
SSO 10g
Database
Oracle Internet Directory
Reregister with OAM 11g
Reverse proxy DAS requests
DAS, and OAM SSO End Point
same_host.domain.com:same_port
Oracle HTTP Server 11g mod_weblogic
WebLogic Server
OAM 11g Servers
Database Policy Store
OID 11g as user identity store

To use this migration scenario, follow the steps listed in Table 14–1.

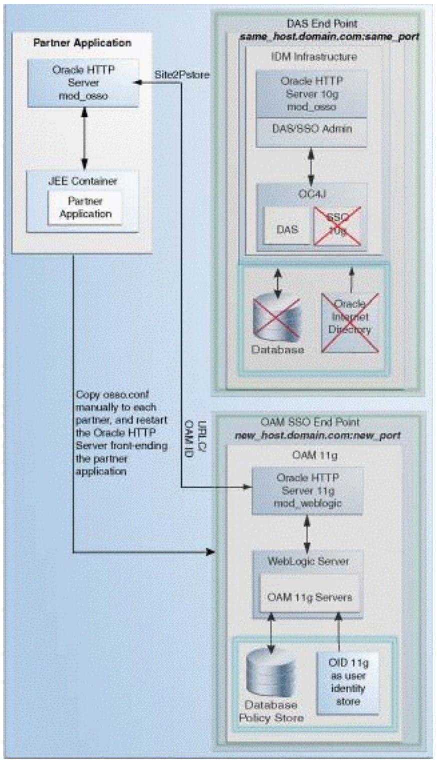
## 14.4.2 Oracle Delegated Administration Services Required, but Oracle Single Sign-On Admin Not Required After Migrating Oracle Single Sign-On to Access Manager 11.1.2

Use this migration scenario if you do not require the Oracle Single Sign-On Admin tool application, but you require the Oracle Delegated Administration Services application after migrating from Oracle Single Sign-On 10*g* to Access Manager 11.1.2. Figure 14–4 illustrates the scenario.

Note the following points when using this migration scenario:

- You are using the OHS 10*g* port for Oracle Delegated Administration Services. Therefore, you must install Access Manager 11.1.2 on a different machine.
- Migrate your partner applications in a phased manner.
- Oracle Single Sign-On will no longer work after the migration. However, Oracle Delegated Administration Services will continue to work.
- You must copy the `osso.conf` files generated during the migration manually for each `OHS/mod_osso` fronting a set of partner applications. This step associates these applications with Access Manager 11.1.2 as their new Oracle Single Sign-On provider. This step is also necessary for Oracle Delegated Administration Services.
- The Oracle Delegated Administration Services endpoint (`same_host.domain.com:same_port`) remains the same for all the partner applications.
- The Oracle Access Manager-Oracle Single Sign-On endpoint is new, such as `new_host.domain.com:new_port`.
- After you perform the migration, Oracle Internet Directory is selected as the user identity store automatically.

***Figure 14–4 Oracle Single Sign-On Administration Server Not required***


Partner Application
Oracle HTTP Server mod_osso
JEE Container
Partner Application
Site2Pstore
DAS End Point
same_host.domain.com:same_port
IDM Infrastructure
Oracle HTTP Server 10g mod_osso
DAS/SSO Admin
OC4J
DAS
SSO 10g
Database
Oracle Internet Directory
Copy osso.conf manually to each partner, and restart the Oracle HTTP Server front-ending the partner application
URL©/ OAM ID
OAM SSO End Point
new_host.domain.com:new_port
OAM 11g
Oracle HTTP Server 11g mod_weblogic
WebLogic Server
OAM 11g Servers
Database Policy Store
OID 11g as user identity store

To use this migration scenario, follow the steps listed in Table 14–1.

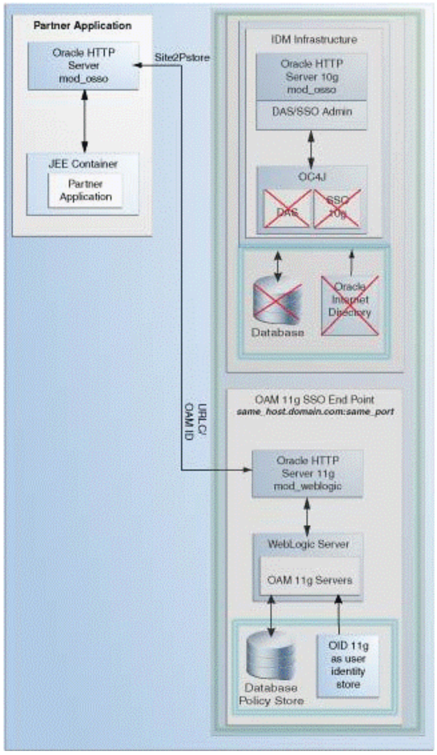
### 14.4.3 Oracle Delegated Administration Services Not Required After Migrating Oracle Single Sign-On to Access Manager 11.1.2

Use this migration scenario if you do not require the Oracle Delegated Administration Services application or the Oracle Single Sign-On Admin tool. Figure 14–5 illustrates the scenario.

Note the following points when using this migration scenario:

- Oracle Single Sign-On and Oracle Delegated Administration Services will no longer work after the migration.
- Migrate all partner applications at once.
- You are using the same OHS 10*g* port that front-ended Oracle Single Sign-On 10*g* as the new port for Access Manager 11.1.2. Therefore, the Oracle Single Sign-On 10*g* server as well as the Oracle Delegated Administration Services application cannot be accessed.
- The Oracle Single Sign-On endpoint (`same_host.domain.com:same_port`) remains the same for all the partner applications.
- After you perform the migration, Oracle Internet Directory is selected as the user identity store automatically.

***Figure 14–5 Oracle Delegated Administration Services Not Required***



To use this migration scenario, follow the steps listed in Table 14–1.

## 14.5 Migration Roadmap

Table 14–1 describes the tasks that should be completed for each of the Oracle Single Sign-On 10*g* migration scenarios.

***Table 14–1 Migration Scenarios and Tasks***

| Scenario | Tasks to be Completed |
|---|---|
| Oracle Delegated Administration Services Required After Migrating Oracle Single Sign-On 10g to Access Manager 11.1.2 | ■ Section 14.6, "Prerequisites for Migration"<br>■ Section 14.7, "Understanding the Access Manager 11.1.2 Topology"<br>■ Section 14.8, "Optional: Upgrading the Oracle Database"<br>■ Section 14.9, "Creating Schemas Using Repository Creation Utility"<br>■ Section 14.10.1, "Installing and Configuring Access Manager 11.1.2 Using Oracle Single Sign-On 10g Host Name and Port Number"<br>■ Section 14.11, "Upgrading Access Manager 11.1.2 Middle Tier Using Upgrade Assistant"<br>■ Section 14.12, "Post-Migration Tasks"<br>■ Section 14.13, "Verifying the Migration" |
| Oracle Delegated Administration Services Required, but Oracle Single Sign-On Admin Not Required After Migrating Oracle Single Sign-On to Access Manager 11.1.2 | ■ Section 14.6, "Prerequisites for Migration"<br>■ Section 14.7, "Understanding the Access Manager 11.1.2 Topology"<br>■ Section 14.8, "Optional: Upgrading the Oracle Database"<br>■ Section 14.9, "Creating Schemas Using Repository Creation Utility"<br>■ Section 14.10.2, "Installing and Configuring Access Manager 11.1.2 Using New Host Name or New Port Number"<br>■ Section 14.11, "Upgrading Access Manager 11.1.2 Middle Tier Using Upgrade Assistant"<br>■ Section 14.12, "Post-Migration Tasks"<br>■ Section 14.13, "Verifying the Migration" |
| Oracle Delegated Administration Services Not Required After Migrating Oracle Single Sign-On to Access Manager 11.1.2 | ■ Section 14.6, "Prerequisites for Migration"<br>■ Section 14.7, "Understanding the Access Manager 11.1.2 Topology"<br>■ Section 14.8, "Optional: Upgrading the Oracle Database"<br>■ Section 14.9, "Creating Schemas Using Repository Creation Utility"<br>■ Section 14.10.1, "Installing and Configuring Access Manager 11.1.2 Using Oracle Single Sign-On 10g Host Name and Port Number"<br>■ Section 14.11, "Upgrading Access Manager 11.1.2 Middle Tier Using Upgrade Assistant"<br>■ Section 14.12, "Post-Migration Tasks"<br>■ Section 14.13, "Verifying the Migration" |

## 14.6 Prerequisites for Migration

You must complete the following prerequisites for migrating Oracle Single Sign-On 10*g* to Access Manager 11.1.2:

1. Read the Oracle Fusion Middleware System Requirements and Specifications document to ensure that your environment meets the minimum requirements for the products you are installing, upgrading, and migrating.

   **Note:** For information about Oracle Fusion Middleware concepts and directory structure, see "Understanding Oracle Fusion Middleware Concepts and Directory Structure" in the *Oracle Fusion Middleware Installation Planning Guide for Oracle Identity and Access Management*.

2. Verify that the Oracle Single Sign-On 10*g* version that you are using is supported for migration. For information about supported starting points for Oracle Single Sign-On 10*g* migration, see Section 11.4, "Supported Starting Points for Oracle Single Sign-On 10g Migration".

## 14.7 Understanding the Access Manager 11.1.2 Topology

Before you begin the migration process, get familiar with the topology of Access Manager 11.1.2.

For more information, see Section 14.3, "Topology Comparison".

## 14.8 Optional: Upgrading the Oracle Database

When you are migrating an Oracle Single Sign-On environment to Access Manager 11.1.2, you must ensure that the version of the database where you plan to install the Access Manager and Oracle Platform Security Services (OPSS) schemas is supported by Oracle Fusion Middleware 11g.

You can install a new database, or upgrade your existing database to a supported version.

## 14.9 Creating Schemas Using Repository Creation Utility

You must create the necessary schemas in the database in order to configure Access Manager 11.1.2. To create schemas, you must run the Repository Creation Utility (RCU). However, you do not need to create all the schemas specified in the RCU, unless you plan to install a complete Oracle Fusion Middleware environment and you plan to use the same database for all the Oracle Fusion Middleware component schemas.

For more information about the running the RCU to create necessary schemas for Access Manager 11.1.2, see "Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU)" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.:

## 14.10 Installing and Configuring the Access Manager 11.1.2 Middle Tier

Depending on the migration scenario you choose, you must complete one of the following tasks:

- Installing and Configuring Access Manager 11.1.2 Using Oracle Single Sign-On 10g Host Name and Port Number

- Installing and Configuring Access Manager 11.1.2 Using New Host Name or New Port Number

### 14.10.1 Installing and Configuring Access Manager 11.1.2 Using Oracle Single Sign-On 10*g* Host Name and Port Number

Table 14–2 lists the steps to install and configure the Access Manager 11.1.2 middle tier for using the Oracle Delegated Administration Services application and the Oracle Single Sign-On Admin tool after migrating from Oracle Single Sign-On 10*g* to Oracle Access Manager 11.1.2.

***Table 14–2 Steps to Install and Configure the Oracle Access Manager Middle Tier***

| No | Task | For More Information |
|---|---|---|
| 1 | Installing Oracle WebLogic Server 10.3.6, and Creating the Oracle Middleware Home | See, "Preparing for Installation" and "Running the Installation Program in Graphical Mode" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*. |
| 2 | Stopping and Configuring the Oracle HTTP Server 10g | See, Reconfiguring Oracle HTTP Server 10g. |
| 3 | Installing Oracle HTTP Server 11*g* | Install Oracle HTTP Server 11*g* and specify the Oracle HTTP Server 10*g* port number. For more information, see *Oracle Fusion Middleware Installation Guide for Oracle Web Tier*. |
| 4 | Installing Oracle Identity and Access Management 11.1.2 | See, "Installing Oracle Identity and Access Management (11.1.2)" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*. |
| 5 | Configuring Oracle Access Management Access Manager 11.1.2. | See, "Configuring Oracle Access Management" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*. |
| 6 | Configuring Node Manager to Start Managed Servers | See, "Configuring Node Manager to Start Managed Servers" in the *Oracle Fusion Middleware Administrator's Guide*. |
| 7 | Starting the Oracle WebLogic Server domain | See, section "Starting the Stack" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*. |
| 8 | Front-ending the Access Manager 11.1.2 Managed Server with the Oracle HTTP Server 11g | See, Front-Ending Access Manager 11.1.2 Managed Server with Oracle HTTP Server 11g |
| 9 | Registering the Oracle HTTP Server 10g as a Partner Application | See, Registering Your Applications as Partner Applications of Oracle Access Manager 11g. |
| 10 | Redirecting the OIDDAS Request to the Oracle HTTP Server 10g server | See, Redirecting the Partner Application Request to Oracle HTTP Server 10g server. |
| 11 | Verifying the installation | See, "Verifying the Oracle Access Management Installation" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*. |

#### Reconfiguring Oracle HTTP Server 10*g*

Perform the following steps:

1. Open the `httpd.conf` file from the directory *`ORACLE_HOME`*`\Apache\Apache\conf` on Windows, or *`ORACLE_HOME`*`/Apache/Apache/conf` (on UNIX) in a text editor and change the existing port number to a new port number.
2. Stop Oracle HTTP Server 10*g* by running the `opmnctl` command-line tool (located at `ORACLE_HOME\opmn\bin`) as follows:

   ```
   opmnctl stopproc ias-component=<name_of_the_OHS_instance>
   ```

3. Restart Oracle HTTP Server 10*g* by running the following `opmnctl` commands:

   ```
   OHS_INSTANCE_HOME/bin/opmnctl stopall
   OHS_INSTANCE_HOME/bin/opmnctl startall
   ```

#### Front-Ending Access Manager 11.1.2 Managed Server with Oracle HTTP Server 11*g*

You must use `mod_wl_ohs` to front-end Access Manager 11.1.2 Managed Server with Oracle HTTP Server 11*g*. To do so, complete the following steps:

1. Open the `mod_wl_ohs.conf` file from the directory *`OHS_INSTANCE_HOME`*`/config/OHS/`*`ohs_instance_name`* (On UNIX), or *`OHS_INSTANCE_HOME`*`\config\OHS\`*`ohs_instance_name`* (on Windows) in a text editor, and edit as follows:

   ```
   <IfModule weblogic_module>
                WebLogicHost <OAM Managed Server Host>
                WebLogicPort <OAM Managed Server Port>
                Debug ON
               WLLogFile /tmp/weblogic.log
              MatchExpression *.jsp
         </IfModule>
         <Location />
               SetHandler weblogic-handler
               PathTrim /
               ErrorPage  http://WEBLOGIC_HOST:WEBLOGIC_PORT/
         </Location>
   ```

2. Restart Oracle HTTP Server 11*g* by running the following `opmnctl` commands from the location *`ORACLE_INSTANCE`*`\bin` directory on Windows, or *`ORACLE_INSTANCE`*`/bin` directory on UNIX:

   ```
   opmnctl stopall
   opmnctl startall
   ```

3. Open the `oam-config.xml` file from the *`MW_HOME`*`\user_projects\domains\`*`domain_name`*`\config\fmwconfig` directory on Windows, or *`MW_HOME`*`/user_projects/domains/`*`domain_name`*`/config/fmwconfig` directory on UNIX in a text editor, and edit the `serverhost` and `serverport` entries, as shown in the following example:

   ```
   <Setting Name="OAMSERVER" Type="htf:map">
      <Setting Name="serverhost" Type="xsd:string"><OHS 11G HOST></Setting>
      <Setting Name="serverprotocol" Type="xsd:string">http</Setting>
      <Setting Name="serverport" Type="xsd:string"><OHS 11G PORT></Setting>
      <Setting Name="MaxRetryLimit" Type="xsd:integer">5</Setting>
   </Setting>
   ```

4. Restart the WebLogic Administration Server and the Access Manager 11.1.2 Managed Servers by completing the following tasks:

   a. Stop the WebLogic Administration Server.

b. Stop the Access Manager Managed Servers.

c. Start the WebLogic Administration Server.

d. Start the Access Manager Managed Servers.

For more information about starting and stopping the servers, see "Starting and Stopping Administration Servers" and "Starting and Stopping Managed Servers" in the *Oracle Fusion Middleware Administrator's Guide*.

### Registering Your Applications as Partner Applications of Oracle Access Manager 11*g*

You must register the Oracle Internet Directory and Oracle Delegated Administration Services deployed on Oracle HTTP Server 10*g* partners with Access Manager 11.1.2. To do so, complete the following steps:

1. Log in to the Oracle Access Management 11.1.2 console.
2. Click the **System Configuration** tab.
3. In the **Welcome** page, select **Add OSSO Agents**.
4. In the **Create OSSO Agent** page, enter the following details:
   - **Agent Name**: The identifying name for the `mod_osso` Agent.
   - **Agent Base URL**: The required protocol, host, and port of the computer on which the Web server for the agent is installed. For example, `http://ohs_host:ohs_port`
5. Click **Apply**.

   The agent is created and the `osso.conf` file is generated at *`DOMAIN_HOME`*`/output/`*`AGENT_NAME`* (on UNIX) and *`DOMAIN_HOME`*`\output\`*`AGENT_NAME`* (on Windows).
6. Copy the newly generated agent file to Oracle HTTP Server 10*g* at *`OHS_Config`*`\osso`.
7. Restart Oracle HTTP Server 10*g* by running the following `opmnctl` commands:

```
OHS_INSTANCE_HOME/bin/opmnctl stopall
OHS_INSTANCE_HOME/bin/opmnctl startall
```

### Redirecting the Partner Application Request to Oracle HTTP Server 10*g* server

You must use `mod_proxy` to redirect Oracle Internet Directory and Oracle Delegated Administration Services requests to Oracle HTTP Server 10*g*.

Open the Oracle HTTP Server 11*g* `httpd.conf` file in a text editor and add entries of OHS 10*g* host name and post name front-ending Oracle Internet Directory and Oracle Delegated Administration Services, as shown in the following example:

```
ProxyPass         /oiddas http://pdcasqa14-3.us.abc.com:8888/oiddas
ProxyPassReverse  /oiddas http://pdcasqa14-3.us.abc.com:8888/oiddas
```

**Note:** The above example is using the OHS 10*g* port number.

Restart Oracle HTTP Server 11*g* by running the following `opmnctl` commands:

```
ORACLE_HOME/opmn/bin/opmnctl stopall
```

```
ORACLE_HOME/opmn/bin/opmnctl startall
```

If your Oracle HTTP Server 10*g* is SSL enabled, you must complete the following:

1. Create a wallet for the proxy.
2. If the root certificate of Oracle HTTP Server 10*g* is not well-known, you must import it into the above created wallet as a trusted certificate.
3. Open the Oracle HTTP Server 11*g* `ssl.conf` file (located in `<ORACLE_INSTANCE>/config/OHS/<COMPONENT_NAME>/`) in a text editor and add the following line under `<VirtualHost *:PORTNUMBER><IfModule ossl_module>`:

   ```
   SSLProxyEngine On
   SSLProxyWallet <PATH of the wallet created above>
   ```

4. Restart Oracle HTTP Server 11*g* by running the following `opmnctl` commands:

   ```
   OHS_INSTANCE_HOME/bin/opmnctl stopall
   OHS_INSTANCE_HOME/bin/opmnctl startall
   ```

### 14.10.2 Installing and Configuring Access Manager 11.1.2 Using New Host Name or New Port Number

Table 14–3 lists the steps you must perform when installing and configuring the Access Manager 11.1.2 middle tier, using a new host name or port number for Oracle Access Manager.

***Table 14–3 Steps to Install and Configure the Oracle Access Manager Middle Tier***

| No | Task | For More Information |
|---|---|---|
| 1 | Installing Oracle WebLogic Server 10.3.6, and Creating the Oracle Middleware Home | See, "Preparing for Installation" and "Running the Installation Program in Graphical Mode" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*. |
| 2 | Installing Oracle Identity and Access Management 11*g* Release 2 (11.1.2) | See, "Installing Oracle Identity and Access Management (11.1.2)" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*. |
| 3 | Configuring Oracle Access Management Access Manager 11.1.2 | See, "Configuring Oracle Access Management" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*. |
| 4 | Configuring Node Manager to Start Managed Servers | See, "Configuring Node Manager to Start Managed Servers" in the *Oracle Fusion Middleware Administrator's Guide*. |
| 5 | Starting the Oracle WebLogic Server domain | See, section "Starting the Stack" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*. |
| 6 | Verifying the installation | See, "Verifying the Oracle Access Management Installation" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*. |

## 14.11 Upgrading Access Manager 11.1.2 Middle Tier Using Upgrade Assistant

When you install Access Manager 11.1.2, Upgrade Assistant is installed automatically into the `bin` directory of your Oracle home.

You run Upgrade Assistant once for each Oracle home that you are upgrading. For example, if you are upgrading two different 10*g* Release 2 (10.1.2) Oracle homes that are part of the same 10*g* Release 2 (10.1.2) farm, then you must run Upgrade Assistant two times, once for each of the 10*g* Release 2 (10.1.2) Oracle homes.

To upgrade the middle tier, complete the following steps:

1. Launch the Upgrade Assistant by doing the following:

   **On UNIX**:

   a. Move from your present working directory to the *MW_HOME*/*IAM_HOME*/bin directory using the following command:

   ```
   cd MW_HOME/IAM_HOME/bin
   ```

   b. Run the following command:

   ```
   ./ua
   ```

   **On Windows**:

   a. Move from the present working directory to the *MW_HOME*\*IAM_HOME*\\bin directory using the following command on the command line:

   ```
   cd MW_HOME\IAM_HOME\bin
   ```

   b. Run the following command:

   ```
   ua.bat
   ```

   The Oracle Fusion Middleware Upgrade Assistant **Welcome** screen is displayed.

2. Click **Next**.

   The **Specify Operation** screen is displayed.

3. Select **Upgrade Oracle Access Manager Middle Tier**.

   The options available in Upgrade Assistant are specific to the Oracle home from which it started. When you start Upgrade Assistant from an Oracle Application Server Identity Management Oracle home, the options shown on the Specify Operation screen are the valid options for an Oracle Application Server Identity Management Oracle home.

4. Click **Next**.

   The **Specify Source Details** screen is displayed.

5. Enter the following information:

   - **Properties File**: Click **Browse** and specify the path to the Oracle Single Sign-On 10*g* `policy.properties` file.

     If your Oracle Access Manager 11.1.2 installation is on a separate host from the Oracle Single Sign-On 10*g* installation, you must copy the 10*g* `policy.properties` file to a temporary directory on the Access Manager 11.1.2 host. Then specify the path to the `policy.properties` file located in your temporary folder.

- **Database Host**: Enter the database host name that contains the Oracle Single Sign-On schema.
- **Database Port**: Enter the database port number.
- **Database Service**: Enter the database service name.
- **SYS Password**: Enter the password for the SYS database account of the database that you selected from the Database drop-down menu. Upgrade Assistant requires these login credentials before it can upgrade the 10*g* components schemas.

> **Note:** Ensure that you enter database details for the Oracle Single Sign-On 10*g* database configuration.

6. Click **Next**.

   The **Specify OID Details** screen is displayed.

7. Enter the following information:

   - **OID Host**: Enter the host name of the Oracle Internet Directory server.
   - **OID SSL Port**: Enter your Oracle Internet Directory port number.
   - **OID Password**: Enter the password for the Oracle Internet Directory administration account (`cn=orcladmin`).

8. Click **Next**.

   The **Specify WebLogic Server** screen is displayed.

9. Enter the following information:

   - **Host**: Enter the host name of the Oracle WebLogic Server domain.
   - **Port**: Enter the listening port of the Administration Server. The default server port is `7001`.
   - **Username**: The user name that is used to log in to the Administration Server. This is the same user name you use to log in to the Administration Console for the domain.
   - **Password**: The password for the administrator account that is used to log in to the Administration Server. This is the same password you use to log in to the Administration Console for the domain.

10. Click **Next**.

    The **Specify Upgrade Options** screen is displayed

11. Select **Start destination components after successful upgrade**, and click **Next**.

    > **Note:** If you are using external application, select **Upgrade even with external applications**.

    The **Examining Components** screen is displayed.

12. Click **Next**.

    The **Upgrade Summary** screen is displayed.

13. Click **Upgrade**.

The **Upgrade Progress** screen is displayed. This screen provides the following information:

- The status of the upgrade
- Any errors or problems that occur during the upgrade

14. Click **Next**.

    The **Upgrade Complete** screen is displayed. This screen confirms that the upgrade was complete.

15. Click **Close**.

## 14.12 Post-Migration Tasks

The following sections describe the manual steps that you must perform after migrating Oracle Single Sign-On 10*g* to Access Manager 11.1.2:

- Configuring Oracle Internet Directory Delegated Administration Services (If Required)
- Configuring Oracle Portal 10g with Access Manager 11.1.2 Server if the Oracle HTTP Server Port is Changed
- Configuring Oracle Access Management 11.1.2 Administration Console to Align Roles
- Copying the osso.conf File
- Configuring Oracle Business Intelligence Discoverer 11g with Access Manager 11.1.2
- Setting the Headers in the Authentication Policy for the Protected DAS Resources
- Setting the Default Authentication Scheme
- Setting the Migrated Identity Store as Default Store and System Store for Access Manager 11.1.2
- Additional Step for Oracle Internet Directory Configured in SSL Server Authentication Mode
- Additional Access Manager Post-Migration Tasks
- Decommissioning Oracle Single Sign-On 10g

### 14.12.1 Configuring Oracle Internet Directory Delegated Administration Services (If Required)

Complete the following steps if you wish to configure Oracle Internet Directory Delegated Administration Services (OIDDAS), after you migrate Oracle Single Sign-On 10*g* to Access Manager 11.1.2:

1. OIDDAS is only supported for customers with current Oracle Portal, or Oracle Forms and Reports license. To obtain the OIDDAS patch, raise a service request (SR).
2. Apply the patch by following the instructions described in the ReadMe file that is available with the patch.
3. Deploy `oiddas.war` against `oam-servers/oam-cluster` on a WebLogic container. The `oiddas.war` file can be found at the following location:

   **On UNIX**: `IDM_HOME/oam/server/apps/oiddas.war`

**On Windows**: *IDM_HOME*`\oam\server\apps/oiddas.war`

4. Register the `mod_osso` agent with Access Manager 11.1.2. This creates a policy and resource. The resource should refer to `/oiddas/**`, and it should be protected by **LDAPscheme**.

   For more information about registering OSSO agent with Access Manager, see "Registering OSSO Agents Using Oracle Access Management Console" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.

   Ensure that you have copied `osso.conf` file from the location *DOMAIN_HOME*`/output/`*Agent_Name* to the location *WebTier_HOME*`/instances/`*Instance_Name*`/config/OHS/ohs1/config/` on the host where Oracle HTTP Server is running.

5. In Access Manager 11.1.2, add responses of type header in authentication policy for protecting DAS resource:

   ```
   osso-subscriber                DEFAULT COMPANY
   ```

   ```
   osso-subscriber-dn            dc=example,dc=mycompany,dc=com (the DN of
   subtree)
   ```

   ```
   osso-subscriber-guid          9B49B4DCF822A78EE040E50AD98369EA  (actual
   orclguid for 'dc=example,dc=mycompany,dc=com')
   ```

   The values for `osso-subscriber-dn` and `osso-subscriber-guid` depends on your configuration.

   For more information about adding a policy response, see "Adding a Policy Response for SSO" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.

6. In OHS, edit the `mod_osso.conf` file at the location *ORACLE_PORTAL_INSTANCE_HOME*`/config/OHS/ohs1/moduleconf/mod_osso.conf`, to protect `"oiddas/ui/oracle/ldap/das"`, as shown in the following example:

   ```
   <Location /oiddas/ui/oracle/ldap/das>
          require valid-user
          AuthType Osso
   </Location>
   ```

7. In Oracle Portal, edit the `mod_wl_ohs` file at the location *ORACLE_PORTAL_INSTANCE_HOME*`/config/OHS/ohs1/mod_wl_ohs.conf` as shown in the following example:

   ```
         <IfModule weblogic_module>
           WebLogicHost weblogic_hostname
           WebLogicPort weblogic_port
   #       Debug ON
   #       WLLogFile /tmp/weblogic.log
   #       MatchExpression *.jsp
         </IfModule>

         <Location /oiddas>
           SetHandler weblogic-handler
           PathTrim /weblogic
   #       ErrorPage  http:/WEBLOGIC_HOME:WEBLOGIC_PORT/
         </Location>
   ```

8. Configure OID IDstore in Access Manager 11.1.2 if it is not configured already. If OID is already configured with Access Manager, skip this step.

For information about configuring new identity store in Access Manager, see "Registering a New User Identity Store" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.

9. Change the Ldap module (Authentication Module) to use newly created IDstore.

   For information about editing the LDAP module, see "Viewing or Editing Native Authentication Modules" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.

10. Modify `das.properties` file at the location `OAM_DOMAIN_HOME/config/fmwconfig` to add OID connection details.

    The following example shows the OID connection details that you must specify in the `das.properties` file.

    ```
    APPLICATION_PRINCIPAL|cn=companyadmin
    APPLICATION_CREDENTIALS|secret
    HOST_NAME|example.mycompany.com
    PORT_NUMBER|port
    USER_PRINCIPAL|cn=companyadmin
    USER_CREDENTIALS|secret
    USER_NAME|username
    SSL_ENABLED|false
    DEBUG|false
    DEBUG_LEVEL|session
    DIAGNOSTIC|false
    INIT_POOLSIZE|10
    LOCAL_TESTING|true
    DEFAULT_CONSOLE|oiddashome
    SUBSCRIBER_NAME|name
    SUBSCRIBER_PRINCIPAL|dc=example,dc=mycompany,dc=com
    ```

11. Restart the WebLogic Administration Server and the Access Manager 11.1.2 Managed Servers by completing the following tasks:

    a. Stop the WebLogic Administration Server.

    b. Stop the Access Manager Managed Servers.

    c. Start the WebLogic Administration Server.

    d. Start the Access Manager Managed Servers.

    For more information about starting and stopping the servers, see "Starting and Stopping Administration Servers" and "Starting and Stopping Managed Servers" in the *Oracle Fusion Middleware Administrator's Guide*.

### 14.12.2 Configuring Oracle Portal 10*g* with Access Manager 11.1.2 Server if the Oracle HTTP Server Port is Changed

After migrating the Oracle Portal's Oracle Single Sign-On Server to the Access Manager 11.1.2 Server, you must update the Oracle Portal schema with information about the Access Manager 11.1.2 server. To do so, you must update the `wwsec_enabler_config_info$` table as follows:

1. Retrieve the Portal schema password by running the following command:

   ```
   ldapsearch -v -D "cn=orcladmin" -w "orcladminpassword" -h OIDHost -p OIDPort -s
   sub -b "cn=IAS  Infrastructure Databases, cn=IAS, cn=Products,
   cn=OracleContext" "orclresourcename=PORTAL"  orclpasswordattribute
   ```

2. Connect to the database hosting the Oracle Portal schema, and log in with the Portal schema user name and password.
3. Run the `portal_post_upgrade.sql` script (located at `<ORACLE_HOME>\oam\server\upgrade\sql`).
4. When prompted, enter your Access Manager 11.1.2 Managed Server host name and port number.

### 14.12.3 Configuring Oracle Access Management 11.1.2 Administration Console to Align Roles

After migration, the Oracle Access Management 11.1.2 Administration console uses the system identity store for run-time authentication and authorization. To align the existing roles, do the following:

1. Run the following command to launch the WebLogic Scripting Tool (WLST):

   **On UNIX**:

   a. Move from your present working directory to the *IAM_HOME*`/common/bin` directory by running the following command on the command line:

      ```
      cd IAM_HOME/common/bin
      ```

   b. Run the following command to launch the WebLogic Scripting Tool (WLST):

      ```
      ./wlst.sh
      ```

   **On Windows**:

   a. Move from your present working directory to the *IAM_HOME*`\common\bin` directory by running the following command on the command line:

      ```
      cd IAM_HOME\common\bin
      ```

   b. Run the following command to launch the WebLogic Scripting Tool (WLST):

      ```
      wlst.cmd
      ```

2. In the WLST shell, enter the following command:

   ```
   editUserIdentityStore(name="UserIdentityStoreName",roleSecAdmin="SecurityAdminR
   oleName")
   ```

   Example:

   ```
   (name="MigratedUserIdentityStore",roleSecAdmin="Administrators")
   ```

If you want to configure a group for Access Manager 11.1.2 Administrator for the Oracle Access Management 11.1.2 Administration console, complete the following steps:

1. Create a group for example Administrators in the Oracle Internet Directory.
2. Add the fully qualified domain name for Access Manager 11.1.2 Administrator privileges. For example, enter the following as the unique member of the group:

   ```
   cn=orcladmin,cn=users,dc=us,dc=abc,dc=com
   ```

3. Run the following command to launch the WebLogic Scripting Tool (WLST):

   **On UNIX**:

   a. Move from your present working directory to the *IAM_HOME*`/common/bin` directory by running the following command on the command line:

```
cd IAM_HOME/common/bin
```

b. Run the following command to launch the WebLogic Scripting Tool (WLST):

```
./wlst.sh
```

**On Windows**:

a. Move from your present working directory to the `IAM_HOME\common\bin` directory by running the following command on the command line:

```
cd IAM_HOME\common\bin
```

b. Run the following command to launch the WebLogic Scripting Tool (WLST):

```
wlst.cmd
```

4. In the WLST shell, enter the following command:

```
editUserIdentityStore(name="MigratedUserIdentityStore",roleSecAdmin="SecurityAd
minRoleName")
```

Example:

```
editUserIdentityStore(name="MigratedUserIdentityStore",roleSecAdmin="Administra
tors")
```

## 14.12.4 Copying the osso.conf File

Depending on the upgrade scenario selected, the Oracle Upgrade Assistant may generate a new file named `osso.conf` for each partner application in the *Oracle_Home*`/upgrade/temp` directory. You must copy this `osso.conf` file to the location of the partner application registered with Oracle Access Manager 11.1.2.

You must identify the correct `osso.conf` file associated with the partner application.

Example:

```
F78CFE57-dadvmb0097.us.abc.com_22776_769_osso.conf
```

To identify the correct `osso.conf` file, see the `oam-config.xml` file (located at, `IDM_HOME/oam/server/config`). The `oam-config.xml` file provides the partner application details and the Oracle HTTP Server host address and port number.

## 14.12.5 Configuring Oracle Business Intelligence Discoverer 11*g* with Access Manager 11.1.2

After migrating the Oracle Business Intelligence Discoverer's Oracle Single Sign-On server to the Access Manager 11.1.2 server, you must update the Oracle Business Intelligence Discoverer Single Sign-On configuration as follows:

1. Open the `mod_osso.conf` file (Located at, `ORACLE_INSTANCE/config/OHS/<COMPONENT_NAME>/moduleconf` in the Oracle Business Intelligence Discoverer instance) in a text editor.

2. Add the following line in the `<IfModule mod_osso.c>`:

```
OssoHTTPOnly Off
```

3. Restart Oracle HTTP Server by running the following `opmnctl` command:

```
OHS_INSTANCE_HOME/bin/opmnctl stopall
OHS_INSTANCE_HOME/bin/opmnctl startall
```

### 14.12.6 Setting the Headers in the Authentication Policy for the Protected DAS Resources

After migration, you must set the headers in the authentication policy for protected Oracle Delegated Administration Services using the Oracle Access Management 11.1.2 console. To do this, complete the following steps:

1. Log in to the Oracle Access Management 11.1.2 console using the following URL:

   ```
   http://host:port/oamconsole
   ```

   In this URL,

   - `host` refers to the fully qualified domain name of the machine hosting the Oracle Access Management 11.1.2 console
   - `port` refers to the designated bind port for the Oracle Access Management 11.1.2 console, which is the same as the bind port for the Administration Server

2. Go to the **Policy Configuration** tab.
3. Expand **Application Domains**.
4. Expand the *agent* that you created while performing the step Registering Your Applications as Partner Applications of Oracle Access Manager 11g.
5. Expand **Authentication Policies**.
6. Double-click on **Protected Resource Policy**.
7. Go to the **Responses** tab in the Protected Resource Policy page.
8. Click on the **+** symbol, to add responses.
9. Add the three headers listed in Table 14–4 with the right values for **Name**, **Type**, and **Value** fields as specified in the table. Click **Add** after adding each header.

*Table 14–4 Headers to be Added*

| Header Name | Type | Value |
|---|---|---|
| osso-subscriber | Header | *DEFAULT COMPANY* |
| osso-subscriber-dn | Header | *DN of subtree*<br>For example:<br>dc=example,dc=mycompany,dc=com |
| osso-subscriber-guid | *Header* | *GUID for the DN* |

10. Restart the WebLogic Administration Server and the Access Manager 11.1.2 Managed Servers by completing the following tasks:

    a. Stop the WebLogic Administration Server.

    b. Stop the Access Manager Managed Servers.

    c. Start the WebLogic Administration Server.

    d. Start the Access Manager Managed Servers.

    For more information about starting and stopping the servers, see "Starting and Stopping Administration Servers" and "Starting and Stopping Managed Servers" in the *Oracle Fusion Middleware Administrator's Guide*.

### 14.12.7 Setting the Default Authentication Scheme

After migration, the default authentication scheme remains to be **LDAPScheme**. You must change this to **SSOCoexistMigrateScheme**. Therefore, after migration, you must set SSOCoexistMigrateScheme as the default authentication scheme using the Oracle Access Management 11.1.2 console. To do this, complete the following steps:

1. Log in to the Oracle Access Management 11.1.2 console using the following URL:

   ```
   http://host:port/oamconsole
   ```

   In this URL,

   - `host` refers to the fully qualified domain name of the machine hosting the Oracle Access Management 11.1.2 administration console
   - `port` refers to the designated bind port for the Oracle Access Management 11.1.2 console, which is the same as the bind port for the Administration Server

2. Go to the **Policy Configuration** tab.
3. Expand **Shared Components** on the left navigation pane.
4. Expand **Authentication Schemes**.
5. Double-click on **SSOCoexistMigrateScheme**.
6. Click Set as **Default**, and click **Apply**.

### 14.12.8 Setting the Migrated Identity Store as Default Store and System Store for Access Manager 11.1.2

After you migrate Oracle Single Sign-On 10*g* to Access Manager 11.1.2, you must explicitly set the `migratedUserIdentityStore` as the Default Store and System Store for Access Manager 11.1.2. To do this, refer to "Setting the Default Store and System Store" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.

### 14.12.9 Additional Step for Oracle Internet Directory Configured in SSL Server Authentication Mode

If the Oracle Internet Directory (OID) used by Oracle Single Sign-On 10*g* is configured in SSL server authentication mode, you must complete the following steps:

1. Add the Oracle Internet Directory self-signed to the `cacerts` file for the JVM that is running the Access Manager 11.1.2 Server by running the following command:

   ```
   <JRE_HOME>/lib/security > ../../../bin/keytool -import -trustcacerts
   -keystore <location of cacerts in jvm> -storepass changeit -noprompt
   -alias <cert-name> -file <cert-file-path>
   ```

2. Restart the WebLogic Administration Server and the Access Manager 11.1.2 Managed Servers by completing the following tasks:

   a. Stop the WebLogic Administration Server.

   b. Stop the Access Manager Managed Servers.

   c. Start the WebLogic Administration Server.

   d. Start the Access Manager Managed Servers.

For more information about starting and stopping the servers, see "Starting and Stopping Administration Servers" and "Starting and Stopping Managed Servers" in the *Oracle Fusion Middleware Administrator's Guide*.

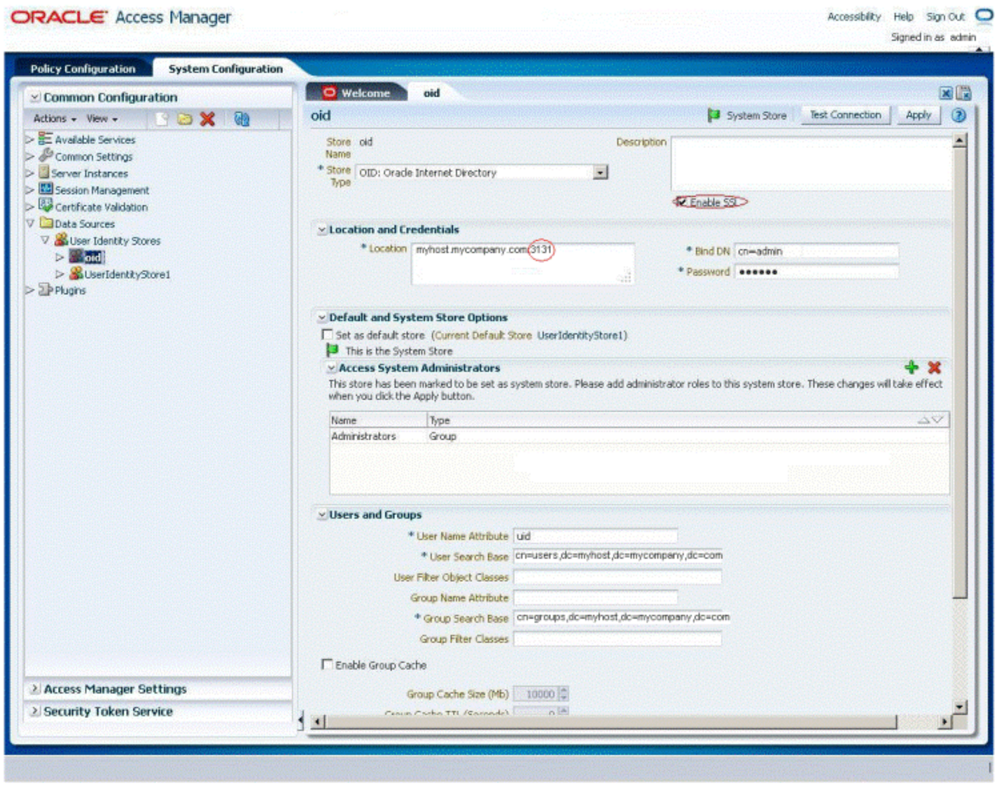
3. Log in to the Oracle Access Management 11.1.2 console using the following URL:

   ```
   http://host:port/oamconsole
   ```

4. Go to the **System Configuration** tab.
5. Expand **Data Sources** under **Common Configuration** on the left navigation pane.
6. Click **User Identity Stores**, and then click **Create**.
7. Specify the required details, and ensure that you select **Enable SSL**.
8. Ensure that you have specified the right SSL port in the **Location** field.
9. Click **Apply**.

Figure 14–6 shows the Access Manager console where you create new User Identity Store.

***Figure 14–6 Creating New User Identity Store***



oid

Store Name: oid

* Store Type: OID: Oracle Internet Directory

Description:

☑ Enable SSL

**Location and Credentials**

* Location: myhost.mycompany.com:3131
* Bind DN: cn=admin
* Password: ••••••

**Default and System Store Options**

□ Set as default store (Current Default Store UserIdentityStore1)

This is the System Store

**Access System Administrators**

This store has been marked to be set as system store. Please add administrator roles to this system store. These changes will take effect when you click the Apply button.

| Name | Type |
|---|---|
| Administrators | Group |

**Users and Groups**

* User Name Attribute: uid
* User Search Base: cn=users,dc=myhost,dc=mycompany,dc=com

User Filter Object Classes:

Group Name Attribute:

* Group Search Base: cn=groups,dc=myhost,dc=mycompany,dc=com

Group Filter Classes:

□ Enable Group Cache

Group Cache Size (Mb): 10000

Group Cache TTL (Seconds): 0

## 14.12.10 Additional Access Manager Post-Migration Tasks

You must perform the following additional post-migration tasks after migrating to Access Manager 11.1.2:

- If the destination topology is front-ended by Oracle HTTP server 11g (installed through the 11*g* companion CD) on the same machine as the source, then you can run Upgrade Assistant from the Oracle HTTP server 11*g* installation directory to migrate the Oracle HTTP server that front-ends Oracle Single Sign-On. In such cases, if you use the Upgrade Assistant retain port option, then no re-association of `mod_osso` partners with Oracle Access Manager is required.

- If you are using Oracle Portal 11*g* that you have migrated from Oracle Portal 10*g*, then you must run the `portal_post_upgrade.sql` script (Located at `Oracle_IDM1/oam/server/upgrade/sql`) to update the Oracle Single Sign-On configuration and to use Access Manager 11.1.2 for Single Sign-On authentication.
- In all other cases, the post-migration step of re-associating `mod_osso` partners with the newly migrated Oracle Access Manager 11.1.2 is required. The `mod_osso` configurations generated as part of the migration can be used for this purpose.
- Before logging in to the Oracle Portal, you must restart Oracle Web Cache by running the following `opmnctl` command (located at `<ORACLE_INSTANCE>\bin` directory on Windows, or `<ORACLE_INSTANCE>/bin` directory on UNIX):

```
opmnctl stopall
opmnctl startall
```

### 14.12.11 Decommissioning Oracle Single Sign-On 10*g*

After migrating to Access Manager 11.1.2, if you are not using Oracle Single Sign-On 10*g* on Oracle Internet Directory 10*g* or Oracle Delegated Administration Services 10*g*, then you can deinstall Oracle Single Sign-On 10*g*. To do so, undeploy the Oracle Single Sign-On 10*g* server from the Oracle Identity Management 10*g* Server (`OC4J_SECURITY`) by running the following command on the command line:

```
java -jar admin_client.jar <uri> <adminId> <adminPassword> -undeploy sso
```

## 14.13 Verifying the Migration

After the migration is complete, the Access Manager will be in the co-existence mode, by default. To verify that your Oracle Access Manager migration was successful:

1. Run the Upgrade Assistant again, and select **Verify Instance** on the Specify Operation screen.

   Follow the instructions on the screen for information on how to verify that specific Oracle Fusion Middleware components are up and running.

2. To verify that Access Manager 11.1.2 Administration Server is up and running, log in to the Oracle Access Management 11.1.2 console using the URL:

   ```
   http://host:port/oamconsole
   ```

   In this URL,

   - *`host`* refers to the fully qualified domain name of the machine hosting the Oracle Access Management 11.1.2 administration console.
   - *`port`* refers to the designated bind port for the Oracle Access Management 11.1.2 console, which is the same as the bind port for the Administration Server.

3. To verify that the Access Manager 11.1.2 Managed Server is up and running, do the following:

   a. Log in to Oracle WebLogic Server Administration Console using the required Administrator credentials.

   b. Expand **Domain Structure** on the left pane, and select **Deployments**.

c. Verify that your Managed Server is listed in the **Summary of Deployments** page.

Alternatively, you can check the migration log file for any error messages or use Fusion Middleware Control to verify that Access Manager 11.1.2 and any other Oracle Identity Management components are up and running in the Oracle Fusion Middleware environment.

For more information, see "Getting Started Using Oracle Enterprise Manager Fusion Middleware Control" in the *Oracle Fusion Middleware Administrator's Guide*.

# 15

# Migrating Sun OpenSSO Enterprise 8.0 Environments

This chapter describes how to migrate Sun OpenSSO Enterprise (OpenSSO Enterprise) 8.0 to Oracle Access Management Access Manager (Access Manager) 11*g* Release 2 (11.1.2).

The chapter contains the following sections:

## 15.1 Migration Overview

This section introduces two tools that are used in the process of migrating Sun OpenSSO Enterprise 8.0 to Oracle Access Manager 11.1.2.

### OpenSSO Agent Assessment Tool

The OpenSSO Agent Assessment Tool reads the agents and policies from the OpenSSO Enterprise server, analyzes which policy elements can be migrated to Access Manager 11.1.2, and generates an assessment report. The generated report provides information on whether the agents can be migrated or not, and whether the policies can be manually migrated, auto-migrated, or semi-migrated based on the Access Manager 11.1.2 policy model.

The assessment tool reads and shows information about OpenSSO Enterprise agent profile, policies, user stores, and authentication stores. It assesses what data can be migrated, and what cannot be migrated to Access Manager 11.1.2, based on the understanding of the artifacts supported in Access Manager 11.1.2.

You can generate the assessment report more than once before you can migrate the OpenSSO Enterprise 8.0 to Access Manager 11.1.2.

**Migration Tool**

The Migration tool migrates the following artifacts of OpenSSO Enterprise 8.0 to Access Manager 11.1.2:

- Agents configuration
- Policies
- User store configuration
- Authentication store configuration

> **Note:** The migration tool and assessment tool do not support connection with the configuration store over the SSL port.

For more information about other migration scenarios, see Section 1.3, "Migration and Coexistence Scenarios".

## 15.2 Modes of Migration

This section describes the two modes of migration that you can perform using the procedure described in this chapter. The following are the two modes of migration:

- Complete Migration
- Delta Migration

### 15.2.1 Complete Migration

Complete Migration migrates all compatible agents, policies, user stores, and authentication stores of OpenSSO Enterprise 8.0 to Access Manager 11.1.2. The migration that you perform for the first time is a complete migration. After the first migration, each next run will be considered as delta migration. Complete migration can be performed only once, and only for the first time.

The fresh migration sets the migration version in the Access Manager 11.1.2 configuration store.

To perform complete migration, follow the procedure described in Migration Roadmap.

> **Note:** If the complete migration fails, you must manually clean up the partially migrated data, before you start performing the complete migration again.

### 15.2.2 Delta Migration

Delta Migration is a mode of migration where you can migrate the newly added artifacts (agents, policies, user stores, and authentication stores) of OpenSSO Enterprise 8.0 to Access Manager 11.1.2. Delta migration is supported only for creation operations.

After the first round of migration (that is, complete migration), every migration that you perform is delta migration.

Each time you perform delta migration, the information about the migration version set by complete migration in the Access Manager 11.1.2 configuration store is retrieved, is incremented by one, and is saved back to the Access Manager 11.1.2 configuration store.

The procedure to perform a delta migration is same as that of a complete migration, and is described in Migration Roadmap.

## 15.3 Migration Summary

This sections summarizes the artifacts of OpenSSO Enterprise 8.0 that are compatible with Access Manager 11.1.2. This section contains the following topics:

- Summary of Migration of Agents
- Summary of Migration of Policies
- Summary of Migration of User Stores
- Summary of Migration of Authentication Stores

### 15.3.1 Summary of Migration of Agents

This section summarizes the migration of agents from OpenSSO Enterprise 8.0 to Access Manager 11.1.2.

- This migration tool migrates the agent configuration and not the agent itself. The following agents are supported for migration:

  **Java EE Agents 3.0**: WebLogic 10.3

  **Web Agents 3.0**: Internet Information Services (IIS) 7.5

- Centralized Agents are migrated to Access Manager 11.1.2. These are the agents that work in **centralized configuration** mode. They store all their configuration details in OpenSSO Enterprise 8.0 server, and read the configuration during agent bootstrap from the OpenSSO Enterprise server over REST call. These agents do not honor local configuration file. After migration, the configuration details of these agents are stored in Access Manager 11.1.2.

- Local agents are migrated with minimal configuration. Local agents are the agents that work in **local configuration** mode. These agents honor the local configuration file only for their own configuration. Only the basic configuration properties like agent ID, agent password, agent base URL of the local agents are stored in the OpenSSO Enterprise 8.0 Server. After migration, these configuration details are stored in the Access Manager 11.1.2 Server.

- Agent migration has the backward compatibility.

- If two or more agents exist with the same name under different realms, the agents are migrated with the name preceded by the realm name.

  For example: If the agent named `j2eeAgent` exists in both `TopRealm` (/) and `SubRealm` (`/>SubRealm`), then these agents are migrated with the name `TopRealm_j2eeAgent` and `SubRealm_j2eeAgent`.

## 15.3.2 Summary of Migration of Policies

This section summarizes the migration of policies from OpenSSO Enterprise 8.0 to Access Manager 11.1.2.

OpenSSO Enterprise 8.0 policies consist of the following four artifacts:

- Rules (resources + actions)
- Subjects
- Conditions
- Response Providers

The policies in the assessment report (`PolicyInfo.txt`), which is generated when you run the OpenSSO Agent assessment tool, are classified into Auto Policies, Semi Policies, and Manual Policies based on the compatibility of the artifacts in Access Manager 11.1.2:

- **Auto Policies**: A policy is regarded as auto policy if all the artifacts of that policy can be mapped to the policy artifacts in Access Manager 11.1.2. All the auto policies can be migrated to Access Manager 11.1.2.
- **Semi Policies**: A policy is regarded as semi policy if some of the artifacts of that policy can be mapped to the policy artifacts in Access Manager 11.1.2. Semi policies are not migrated to Access Manager 11.1.2.
- **Manual Policies**: A policy is regarded as manual policy if none of the artifacts of that policy can be mapped to the policy artifacts of Access Manager 11.1.2. Manual policies are not migrated to Access Manager 11.1.2.

OpenSSO Enterprise 8.0 has two types of policies:

- **Referral Policies**: These policies do not apply to migration.
- **Non-Referral Policies**: These policies are migrated.

### Rules

- An OpenSSO Enterprise policy without a rule is not supported for migration. Such policy is considered invalid.
- Rules that have the actions `GET` and `POST` are only applicable for migration. These rules have the service type as `URL Policy Agent`.
- Rules with other service types such as `Discovery Service` that has the actions `LOOKUP` and `UPDATE`, and service type `Liberty Personal Profile Service` that has the actions `QUERY` and `MODIFY` are not applicable for migration because these actions (which are known as resource operations in Access Manager 11.1.2) are not supported in Access Manager 11.1.2.

### Subjects

Only the subject type `OpenSSO Identity Subject` (user and group) and `Authenticated Users` are supported for migration. These subjects are migrated as part of `Identity Condition` in Access Manager 11.1.2.

### Conditions

- Active Session Time
  - This condition of OpenSSO Enterprise policy is mapped to the attribute `Session Expiry Time` of the AttributeCondition in Access Manager 11.1.2.

  - The attribute `Terminate session` of this condition is ignored during migration as the appropriate mapping of this attribute does not exist in Access Manager 11.1.2.

- Authentication by Module Instance
  - This condition of OpenSSO Enterprise policy is migrated to Access Manager 11.1.2 as `AuthN` scheme, and not as a condition.
  - Table 15–1 lists the authentication modules of OpenSSO Enterprise 8.0 that are migrated and mapped with `AuthN` scheme into Access Manager 11.1.2.

***Table 15–1 Mapping of Authentication Module***

| Authentication Module in OpenSSO Enterprise 8.0 | Authentication Plug-in in Access Manager 11.1.2 |
|---|---|
| Certificate auth module | X509 auth plug-in |
| WindowsDesktopSSO auth module | Kerberos auth plug-in |
| LDAP auth module | LDAP auth plug-in |

- Authentication Level (less than or equal to) and Authentication Level (greater than or equal to)
  - Both the conditions of OpenSSO Enterprise policy are mapped to the session attributes of the `AttributeCondition` with namespace `SESSION` and attribute name `Authentication Level`.
  - Both the conditions are mapped to the AttributeOperator `EQUALS`, as Access Manager 11.1.2 does not have corresponding mapping for `greater then or equal to` and `less than or equal to`. This mapping is done because of the `equals` factor in the policy condition in OpenSSO Enterprise 8.0. Therefore, both the conditions `greater then or equal to` and `less than or equal to` are similar in Access Manager 11.1.2.

    For example, if you migrate an OpenSSO Enterprise 8.0 policy with a condition of authentication level `less than or equal to 5`, the migrated policy in Access Manager 11.1.2 will have the authentication level `equal to 5`.

- Current Session Properties
  - This condition is mapped to the session attributes of the AttributeCondition with namespace `SESSION` and attribute name `Other`, where the key/value will be added as attributes of this condition. This condition in OpenSSO Enterprise 8.0 is multi-valued. Therefore, this condition in Access Manager 11.1.2 has multiple attributes with same name but different values.

- Identity Membership
  - This condition in OpenSSO Enterprise policy is mapped to `Identity condition` in Access Manager 11.1.2.
  - All the unique users or groups from all the subjects, and all the unique users or groups from all the identity membership conditions in OpenSSO Enterprise 8.0 are created as a set of users or groups in one Identity condition in Access Manager 11.1.2.
  - During run-time verification, the ORing is performed between this set of users or groups

- IP Address/DNS Name

  - The condition `IP Address` in OpenSSO Enterprise 8.0 policy is mapped to `IP condition` in Access Manager 11.1.2.
  - The condition `DNS name` is not supported in Access Manager 11.1.2.
- LDAP Filter Condition
  - This condition in OpenSSO Enterprise policy is mapped to `Identity condition` in Access Manager 11.1.2.
  - All the unique LDAP filters from all the LDAP filter conditions in OpenSSO Enterprise 8.0 are created as a set of LDAP filters in one Identity condition in Access Manager 11.1.2.
- Time (day, date, time, and time zone)
  - This condition in OpenSSO Enterprise 8.0 policy is mapped to `Time condition` in Access Manager 11.1.2.
  - The `Time` condition in OpenSSO Enterprise 8.0 contains one of the following values: date, time, day, or time zone; whereas the `Time` condition in Access Manager 11.1.2 contains either time or day. Therefore, the `Time` condition in OpenSSO Enterprise 8.0 containing only the time (start and end time) and day can be mapped to the `Time` condition in Access Manager 11.1.2. All the other cases are ignored.

**Response Providers**

- OpenSSO Enterprise Server or Policy Server sends Identity or User repository attributes (that is, user attributes from any user store) to the agent as response providers. The OpenSSO agent sends these attributes back to the resource or application via Http header, request attribute, or Http cookie according to the configuration of the agent.

  All of the response providers (static as well as dynamic) are migrated from OpenSSO Enterprise 8.0 to Access Manager 11.1.2 with the type Http header.

### 15.3.3 Summary of Migration of User Stores

This section summarizes the migration of user stores from OpenSSO Enterprise 8.0 to Access Manager 11.1.2.

OpenSSO Enterprise has three types of user stores:

- **Active Directory**: This user store can be migrated to Access Manager 11.1.2.
- **Generic LDAPv3**: This user store can be migrated to Access Manager 11.1.2.
- **Sun DS with OpenSSO schema**: This user store cannot be migrated to Access Manager 11.1.2, as no supported data store type is available in 11.1.2.

### 15.3.4 Summary of Migration of Authentication Stores

This section summarizes the migration of authentication stores from OpenSSO Enterprise 8.0 to Access Manager 11.1.2.

The following are the authentication stores in OpenSSO Enterprise 8.0 that can be migrated and mapped to the corresponding authentication modules in Access Manager 11.1.2:

- LDAP in OpenSSO Enterprise 8.0 is mapped to OAM LDAP in Access Manager 11.1.2.

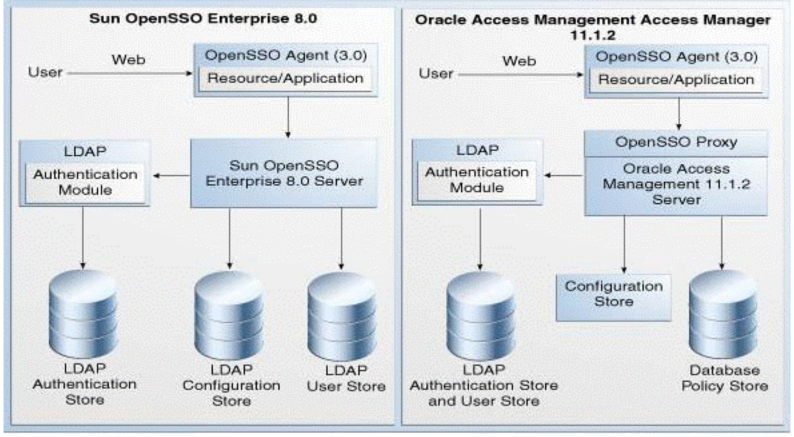
- Certificate in OpenSSO Enterprise 8.0 is mapped to X509 in Access Manager 11.1.2.
- Windows Desktop SSO in OpenSSO Enterprise 8.0 is mapped to Kerberos Access Manager 11.1.2.

All authentication stores with type LDAP are migrated to Access Manager 11.1.2 with name `AS_RealmName_Modulename`. The authentication stores with type other than LDAP are not migrated.

## 15.4 Topology Comparison

Figure 15–1 compares the topologies of Sun OpenSSO Enterprise 8.0 and Access Manager 11.1.2.

***Figure 15–1 OpenSSO Enterprise 8.0 and Access Manager 11.1.2 Topologies***



## 15.5 Migration Roadmap

Table 15–2 lists the steps to migrate Sun OpenSSO Enterprise 8.0 to Access Manager 11.1.2.

***Table 15–2 Task Roadmap***

| Task No | Task | For More Information |
|---|---|---|
| 1 | Complete the prerequisites. | See, Prerequisites for Migration |
| 2 | Install Oracle Identity and Access Management 11.1.2. | See, Installing Oracle Identity and Access Management 11.1.2 |
| 3 | Configure Oracle Access Management Access Manager 11.1.2. | See, Configuring Oracle Access Management Access Manager 11.1.2 |
| 4 | Generate the assessment report, and analyze what artifacts can be migrated to Access Manager 11.1.2.<br>You can perform this task multiple times. | See, Generating the Assessment Report |

*Table 15–2 (Cont.) Task Roadmap*

| Task No | Task | For More Information |
|---|---|---|
| 5 | Start the WebLogic Administration Server. | See, Starting the WebLogic Administration Server |
| 6 | Migrate OpenSSO Enterprise 8.0 to Access Manager 11.1.2 by running the migration tool. | See, Migrating the Artifacts of OpenSSO Enterprise 8.0 to Access Manager 11.1.2 |
| 7 | Complete the post-migration steps. | See, Post-Migration Tasks |
| 8 | Verify the migration. | See, Verifying the Migration |

## 15.6 Prerequisites for Migration

You must complete the following prerequisites for migrating OpenSSO Enterprise 8.0 to Access Manager 11.1.2:

1. Read the Oracle Fusion Middleware System Requirements and Specifications document to ensure that your environment meets the minimum requirements for the products you are installing, upgrading, and migrating.

   **Note:** For information about Oracle Fusion Middleware concepts and directory structure, see "Understanding Oracle Fusion Middleware Concepts and Directory Structure" in the *Oracle Fusion Middleware Installation Planning Guide for Oracle Identity and Access Management*.

2. Verify that the OpenSSO Enterprise version that you are using is supported for migration. For information about supported starting points for OpenSSO Enterprise 8.0 migration, see Section 11.5, "Supported Starting Points for Sun OpenSSO Enterprise Migration".

## 15.7 Installing Oracle Identity and Access Management 11.1.2

As part of migration process, you must freshly install Oracle Identity and Access Management 11.1.2. This 11.1.2 installation can be on the same machine where Sun OpenSSO Enterprise 8.0 is installed, or on a different machine.

For more information about installing Oracle Identity and Access Management 11.1.2, see "Installing Oracle Identity and Access Management (11.1.2)" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

## 15.8 Configuring Oracle Access Management Access Manager 11.1.2

Configure Access Manager 11.1.2, and create a domain.

For information about configuring Access Manager 11.1.2, see "Configuring Oracle Access Management" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

## 15.9 Generating the Assessment Report

This section describes how to generate an assessment report using the OpenSSO Agent assessment tool. This assessment report provides a preview of agents, policies, user stores, and authentication stores that are available in the OpenSSO Enterprise 8.0 Server, and indicates which artifacts can be migrated to Access Manager 11.1.2.

You can generate an assessment report multiple times before you can start the migration process.

This section includes the following topics:

- Obtaining the Assessment Tool
- Specifying LDAP Connection Details
- Running the OpenSSO Agent Assessment Tool
- Analyzing the Assessment Report

> **Note:** Before you run the OpenSSO Agent assessment tool, you must complete the following prerequisites:
>
> - Start the container on which OpenSSO Enterprise 8.0 is deployed.
> - Make sure that you use 1.6 or higher version of JDK.
> - Set the variable `JAVA_HOME` to the appropriate location where JDK 1.6 is installed.

### 15.9.1 Obtaining the Assessment Tool

Move from your present working directory to the *IAM_HOME*`/oam/server/tools/opensso_assessment` directory using the following command:

**On UNIX**:

```
cd IAM_HOME/oam/server/tools/opensso_assessment/
```

**On Windows**:

```
cd IAM_HOME\oam\server\tools\opensso_assessment\
```

Extract the contents of the `OpenssoAgentdiscTool.zip` folder to a directory of your choice. It is recommended that you use the name `OpenssoAgentdiscTool` to the unzipped folder.

### 15.9.2 Specifying LDAP Connection Details

You must specify LDAP connection details in the properties file before you run the OpenSSO Agent assessment tool by doing the following:

1. Open the `OpenSSOAgentDiscTool.properties` file from the following location:

   **On UNIX**: *unzipped_folder*`/resources/`

   **On Windows**: *unzipped_folder*`\resources\`

2. Set the appropriate values for the following properties:

   - `openSSOLDAPServerURL=`*host*`:`*port*

In this property, *host* and *port* refer to the LDAP host and the port of the configuration store used in OpenSSO Enterprise 8.0.

- openSSOLDAPBindDN=*login_id*

  where *login_id* is the bind DN of the LDAP server. You must have the administrative or root permissions to the configuration directory server of OpenSSO Enterprise 8.0.

- openSSOLDAPSearchBase=*LDAP_search_base*

  where *LDAP_search_base* is LDAP search base for the configuration store.

3. Save the file, and close.

> **Note:** if you do not specify the LDAP connection details, a message will be displayed in the UserStoresInfo.txt and AuthnStoreInfo.txt files. This message indicates that the information is not available. The same message will be displayed in the user stores and authentication stores sections in DashBoardInfo.txt file. You must then specify the right LDAP connection details in the OpenSSOAgentDiscTool.properties file, save the file, and run the assessment tool again.
>
> If you specify any incorrect value for any of these parameters, you cannot run the assessment tool, and error is displayed accordingly.

### 15.9.3 Running the OpenSSO Agent Assessment Tool

To run the OpenSSO Agent assessment tool, do the following:

1. Change your directory to the folder where you extracted the contents to, as described in Section 15.9.1, "Obtaining the Assessment Tool", using the following command:

   ```
   cd <path to the unzipped folder>
   ```

2. Run the following command:

   ```
   java -jar openssoagentdisc.jar OpenSSO_server_URL username debugLevel
   ```

   In this command,

   *OpenSSO_server_URL* is the URL of the OpenSSO Enterprise 8.0 Server. You must specify it in the format: http://*host*:*port*/opensso, where *host* and *port* refer to hostname and the port of the machine where OpenSSO Enterprise 8.0 Server is running.

   *username* is the username of the OpenSSO Enterprise 8.0 Server.

   *debugLevel* parameter is optional. The value of this parameter should be either error or message. If you do not specify this parameter in the command, it takes the default value error.

   You are prompted to enter the following:

   1. Enter server login password:

      Enter the password of the OpenSSO Enterprise 8.0 server admin user.

   2. Enter LDAP login password:

      Enter the login password of the LDAP server.

**Note:** For more information about the arguments used in this command, run the following command in the unzipped directory:

```
java -jar openssoagentdisc.jar -help
```

### 15.9.4 Analyzing the Assessment Report

The OpenSSO Agent assessment tool generates five report files in the following location:

```
unzipped_folder/consoleOutput/
```

These reports contain information about agents, policies, user stores, and authentication stores of OpenSSO Enterprise 8.0 that are supported in Access Manager 11.1.2.

Table 15–3 lists the report files that are generated when you run the OpenSSO Agent assessment tool.

***Table 15–3 Report Files Generated***

| File | Description |
|---|---|
| `AgentInfo.txt` | Contains information about J2EE and web agents, and the list of supported agents in Access Manager 11.1.2. |
| `AuthnStoreInfo.txt` | Contains information about authentication stores. |
| `DashBoardInfo.txt` | Contains brief information about agents, policies, user stores, and authentication stores. |
| `PolicyInfo.txt` | Contains information about policies. |
| `UserStoreInfo.txt` | Contains information about user stores. |

## 15.10 Starting the WebLogic Administration Server

You must start the WebLogic Administration Server before you can run the migration tool.

To start the WebLogic Administration Server, do the following:

**On UNIX**:

1. Move from your present working directory to the *`MW_HOME`*`/user_projects/domains/`*`domain_name`*`/bin` directory using the command:

   ```
   cd MW_HOME/user_projects/domains/domain_name/bin/
   ```

2. Run the following command:

   ```
   ./startWebLogic.sh
   ```

   When prompted, enter the username and password of the WebLogic Administration Server.

**On Windows**:

1. Move from your present working directory to the *`MW_HOME`*`\user_projects\domains\`*`domain_name`*`\bin` directory using the following command on the command line:

```
cd MW_HOME\user_projects\domains\domain_name\bin\
```

2. Run the following command:

   ```
   startWebLogic.cmd
   ```

   When prompted, enter the username and password WebLogic Administration Server.

## 15.11 Migrating the Artifacts of OpenSSO Enterprise 8.0 to Access Manager 11.1.2

Before you start the actual migration of the artifacts from OpenSSO Enterprise 8.0 to Access Manager 11.1.2, make sure that you have generated the assessment report (as described in Section 15.9, "Generating the Assessment Report"), and analyzed what artifacts can be migrated to Access Manager 11*g*.

To migrate Sun OpenSSO Enterprise 8.0 to Access Manager 11.1.2, do the following:

1. Create a properties file at any accessible location. For example, create a properties by name `oam_migration.properties`.

   Enter values for the following properties in the properties file:

   - `openSSOServerURL=`*`OpenSSO_server_URL`*
   - `openSSOAdminUser=`*`OpenSSO_admin_username`*
   - `openSSOAdminPassword=`
   - `openSSOServerDebugLevel=error/message`
   - `openSSOLDAPServerURL=`*`LDAP host:port`*
   - `openSSOLDAPBindDN=`*`LDAP_bind_DN`*
   - `openSSOLDAPBindPwd=`
   - `openSSOLDAPSearchBase=`*`LDAP_searchBase`*

   Table 15–4 describes the values you must specify for each of the properties in the properties file.

***Table 15–4 Property File Values***

| Property | Description |
|---|---|
| `openSSOServerURL` | Specify the URL of the OpenSSO Enterprise 8.0 Administration Server. It must be specified in the format:<br>`http://<host>:<port>/opensso`<br>where<br>`<host>` is the machine on which the OpenSSO Enterprise 8.0 Administration Server is running<br>`<port>` is the port number of the OpenSSO Enterprise Administration Server |
| `openSSOAdminUser` | Specify the username of the OpenSSO Enterprise Administration Server. |
| `openSSOAdminPassword` | Do not specify any value for this property. The migration tool prompts you for the OpenSSO Enterprise admin password when you run the migration command, as described in step-4. |

*Table 15–4 (Cont.) Property File Values*

| Property | Description |
|---|---|
| `openSSOServerDebugLevel` | Specify one of the following values:<br>■ `error`<br>■ `message`<br>This value represents the debug level. |
| `openSSOLDAPServerURL` | Specify the URL of the LDAP server. This must be specified in the format:<br>*`host`*`:`*`port`*<br>where<br>*`host`* refers to the LDAP host of the configuration store used in OpenSSO Enterprise 8.0<br>*`port`* refers to the LDAP port of the configuration store used in OpenSSO Enterprise 8.0<br>The *`host`* and *`port`* values must be separated by colon. |
| `openSSOLDAPBindDN` | Specify the bind DN of the LDAP server. This user must have the admin or root permissions to the configuration directory server of OpenSSO Enterprise. |
| `openSSOLDAPBindPwd` | Do not specify any value for this property. The migration tool prompts you for the LDAP bind password when you run the migration command as described in step-4. |
| `openSSOLDAPSearchBase` | Specify the LDAP search base for the configuration store. |

> **Note:** Do not specify any value for `openSSOAdminPassword` and `openSSOLDAPBindPwd` properties.

2. Run the following command to launch the WebLogic Scripting Tool (WLST):

   **On UNIX**:

   a. Move from your present working directory to the *`IAM_HOME`*`/common/bin` directory by running the following command on the command line:

   ```
   cd IAM_HOME/common/bin
   ```

   b. Run the following command to launch the WebLogic Scripting Tool (WLST):

   ```
   ./wlst.sh
   ```

   **On Windows**:

   a. Move from your present working directory to the *`IAM_HOME`*`\common\bin` directory by running the following command on the command line:

   ```
   cd IAM_HOME\common\bin
   ```

   b. Run the following command to launch the WebLogic Scripting Tool (WLST):

   ```
   wlst.cmd
   ```

3. Run the following command to connect WLST to the WebLogic Server instance:

   ```
   connect('wls_admin_username','wls_admin_password','t3://hostname:port');
   ```

   In this command,

*wls_admin_username* is the username of the WebLogic Administration Server.

*wls_admin_password* is the password of the WebLogic Administration Server.

*hostname* is the machine where WebLogic Administration Server ia running.

*port* is the port of the Administration Server.

4. Run the following command to migrate the artifacts of OpenSSO Enterprise 8.0 to Access Manager 11.1.2:

   ```
   oamMigrate(oamMigrateType="OpenSSO",pathMigrationPropertiesFile="absolute_path_
   of_properties_file");
   ```

   In this command,

   *absolute_path_of_properties_file* is the absolute path to the properties file that you created in step-1. For example:

   **On UNIX**:

   ```
   oamMigrate(oamMigrateType="OpenSSO",pathMigrationPropertiesFile="abc/de
   f/oam_migration.properties"
   ```

   **On Windows**:

   ```
   oamMigrate(oamMigrateType="OpenSSO",pathMigrationPropertiesFile="abc\\d
   ef\\oam_migration.properties
   ```

   You are prompted to enter the following:

   1. `Enter value for property : openSSOAdminPassword :`

      Enter the password of the OpenSSO Enterprise 8.0 Administration Server.

   2. `Enter value for property : openSSOLDAPBindPwd :`

      Enter the bind password of the LDAP server.

   **Note:** Complete migration is performed when you run the `oamMigrate()` command for the first time.

   After an initial migration (complete migration), you can re-execute this command to perform delta migration.

   For more information about complete and delta migration, see Section 15.2, "Modes of Migration".

When the migration is complete, the WLST console displays a message stating the result of the migration.

## 15.12 Post-Migration Tasks

After you migrate OpenSSO Enterprise 8.0 to Access Manager 11.1.2, you must complete the following post-migration tasks:

1. The agent artifacts (properties files) are generated when you perform a migration. The following two properties files are generated in the location `domain_home/output/OpenSSOMigration/OpenSSO8.0/Realm_Name/Agent_Name/*.properties`:

   - `OpenSSOAgentBootstrap.properties`
   - `OpenSSOAgentConfiguration.properties`

You must copy these property files to the agents' configuration location. For each agent, complete the following steps:

a. Stop the agent.

b. Back up the existing properties file (that is, the properties file which existed on the agent host before you started the migration process).

c. Copy the agent's artifacts (properties files) to the agent deployment location:

```
/agent_install_dir/weblogic_v10_agent/Agent_001/config
```

d. Modify the container specific property in the `OpenSSOAgentBootstrap.properties` file as follows:

For Glassfish agent, set the following property:

```
com.sun.identity.agents.config.service.resolver=com.sun.identity.agents.app
server.v81.AmASAgentServiceResolver
```

For WebLogic agent, set the following property:

```
com.sun.identity.agents.config.service.resolver=com.sun.identity.agents.web
logic.v10.AmWLAgentServiceResolver
```

e. Restart the agent.

f. Clean up the cookies and cache of the browser.

2. The migration tool does not retrieve the passwords of the user stores that are migrated from OpenSSO Enterprise 8.0 to Access Manager 11.1.2. Therefore, after migration, you must manually update the passwords for all the user stores that are migrated. To do this, complete the following steps:

a. Log in to the Oracle Access Management 11.1.2 console using the following URL:

```
http://host:port/oamconsole
```

In this URL, *host* refers to the fully qualified domain name of the machine hosting the Oracle Access Management Server, and *port* refers to the designated bind port for the Oracle Access Management Console, which is the same as the bind port for the Administration Server.

b. Go to the **System Configuration** tab.

c. Under **Common Configuration**, expand **Data Sources** on the left navigation pane.

d. Expand **User Identity Stores**, manually update the password for all the migrated LDAP user stores that exist.

3. After migration, the minimum and maximum pool size for the migrated authentication stores will be set to 0, by default. Hence, you must manually set the appropriate values for **Minimum Pool Size** and **Maximum Pool Size** for the authentication stores in the Oracle Access Management 11.1.2 console. To do this, complete the following steps:

a. Log in to the Oracle Access Management 11.1.2 console using the URL:

```
http://host:port/oamconsole
```

b. Go to the **System Configuration** tab.

c. Expand **Common Configuration** on the left navigation pane.

d. Expand **Data Sources**, and then expand **User Identity Stores**.

e. Select the authentication store to be edited.

f. Scroll down to **Connection Details**, and set the values **Minimum Pool Size** and **Maximum Pool Size**. For example, Minimum Pool Size=10 and Maximum Pool Size=50.

g. Click **Apply**.

## 15.13 Verifying the Migration

To verify the migration, do the following:

1. Log in to the Oracle Access Management 11.1.2 console using the following URL:

   ```
   http://host:port/oamconsole
   ```

   In this URL,

   - *host* refers to the fully qualified domain name of the machine hosting the Oracle Access Management 11.1.2 console.
   - *port* refers to the designated bind port for the Oracle Access Management 11.1.2 console, which is the same as the bind port for the Administration Server.

   Verify that the OpenSSO Enterprise agents, user stores, authentication stores, authentication modules, host identifiers, resources, policies with correct authentication scheme having correct authentication module are migrated to Access Manager 11.1.2.

2. Access any protected page using the URL. The URL now redirects you to the Oracle Access Management Server login page. Upon successful authentication, it should perform a successful authorization and you should be able to access the resource successfully.

# 16

# Migrating Sun Java System Access Manager 7.1 Environments

This chapter describes how to migrate Sun Java System Access Manager 7.1 to Oracle Access Management Access Manager (Access Manager) 11*g* Release 2 (11.1.2).

The chapter contains the following sections:

## 16.1 Migration Overview

This section introduces two tools that are used in the process of migrating Sun Java System Access Manager 7.1 to Access Manager 11.1.2.

### OpenSSO Agent Assessment Tool

The OpenSSO Agent assessment tool reads the policies from the Sun Java System Access Manager 7.1 server, analyzes which policy elements can be migrated to Access Manager 11.1.2, and generates an assessment report. The generated report provides information on whether the agents can be migrated or not, and whether the policies can be manually migrated, auto-migrated, or semi-migrated based on the Access Manager 11.1.2 policy model.

Assessment tool reads and shows information about Sun Java System Access Manager 7.1 agent profile, policies, user stores, and authentication stores. It assesses what data can be migrated to Access Manager 11.1.2 and what cannot be migrated to Access

Manager 11.1.2 based on the understanding of the supported artifacts in Access Manager 11.1.2.

You can use the assessment tool to generate assessment report more than once before you can migrate the Sun Java System Access Manager 7.1 environment.

#### Migration Tool

The Migration tool migrates the following artifacts of Sun Java System Access Manager 7.1 to Access Manager 11.1.2:

- Agents configuration
- Policies
- User store configuration
- Authentication store configuration

> **Note:** The migration tool and assessment tool do not support connection with configuration store over SSL port.

For more information about other migration scenarios, see Section 1.3, "Migration and Coexistence Scenarios".

## 16.2 Modes of Migration

This section describes the two modes of migration that you can perform using the procedure described in this chapter. The following are the two modes of migration:

- Complete Migration
- Delta Migration

### 16.2.1 Complete Migration

Complete migration migrates all compatible agents, policies, user stores, and authentication stores of Sun Java System Access Manager 7.1 to Access Manager 11.1.2. The migration that you perform for the first time will be a complete migration. After the first migration, each next run will be delta migration. Complete migration can be performed only once, and only for the first time.

The fresh migration sets the migration version in the Access Manager 11.1.2 configuration store through the migration framework.

To perform a complete migration, follow the procedure described in Migration Roadmap.

> **Note:** If the complete migration fails, you must manually clean up the partially migrated data, before you start performing the complete migration again.

### 16.2.2 Delta Migration

Delta migration is a mode of migration where you can migrate the newly added artifacts (agents, policies, user stores, and authentication stores) of Sun Java System Access Manager 7.1 to Access Manager 11.1.2. Delta migration is supported only for creation operations.

After the first round of migration (that is a complete migration), every migration that you perform is delta migration.

Each time you perform delta migration, information about the migration version set by the complete migration in the Access Manager 11.1.2 configuration store is retrieved, is incremented by one, and is saved back to Access Manager 11.1.2 configuration store.

The procedure to perform delta migration is same as that of a complete migration, and is described in Migration Roadmap.

## 16.3 Migration Summary

This sections summarizes the artifacts of Sun Java System Access Manager 7.1 that are compatible with Access Manager 11.1.2. This section contains the following topics:

- Summary of Migration of Agents
- Summary of Migration of Policies
- Summary of Migration of User Stores
- Summary of Migration of Authentication Stores

### 16.3.1 Summary of Migration of Agents

This section summarizes the migration of agents from Sun Java System Access Manager 7.1 to Access Manager 11.1.2.

- This migration tool migrates the agent configuration and not the agent itself. The Web Agent 2.2 supported for migration is Sun Java System Web Server 7.0. The migration tool does not support the migration of J2EE agents.
- Centralized Agents are migrated to Access Manager 11.1.2. These are the agents that work in **centralized configuration** mode. They store all their configuration details in Sun Java System Access Manager 7.1 Server, and read the configuration during agent bootstrap from the Sun Java System Access Manager 7.1 Server over REST call. These agents do not honor local configuration file. After migration, the configuration details of these agents are stored in Access Manager 11.1.2.
- Local agents are migrated with minimal configuration. Local agents are the agents that work in **local configuration** mode. These agents honor the local configuration file only for their own configuration. Only the basic configuration properties like agent ID, agent password, agent base URL of the local agents are stored in the Sun Java System Access Manager 7.1 server. After migration, these configuration details are stored in the Access Manager 11.1.2 Server.
- Agent migration has the backward compatibility.
- If two or more agents exist with the same name under different realms, the agents are migrated with the name preceded by the realm name.

  For example: If the agent named `j2eeAgent` exists in both `TopRealm` (/) and `SubRealm` (`/>SubRealm`), then these agents are migrated with the name `TopRealm_j2eeAgent` and `SubRealm_j2eeAgent`.

### 16.3.2 Summary of Migration of Policies

This section summarizes the migration of policies from Sun Java System Access Manager 7.1 to Access Manager 11.1.2.

Sun Java System Access Manager 7.1 policies consist of the following four artifacts:

- Rules (resources + actions)
- Subjects
- Conditions
- Response Providers

The policies in the assessment report (`PolicyInfo.txt`), which is generated when you run the OpenSSO Agent assessment tool, are classified into Auto Policies, Semi Policies, and Manual Policies based on the compatibility of the artifacts in Access Manager 11.1.2:

- **Auto Policies**: A policy is regarded as auto policy if all the artifacts of that policy can be mapped to the policy artifacts in Access Manager 11.1.2. All the auto policies can be migrated to Access Manager 11.1.2.
- **Semi Policies**: A policy is regarded as semi policy if some of the artifacts of that policy can be mapped to the policy artifacts in Access Manager 11.1.2. Semi policies are not migrated to Access Manager 11.1.2.
- **Manual Policies**: A policy is regarded as manual policy if none of the artifacts of that policy can be mapped to the policy artifacts of Access Manager 11.1.2. Manual policies are not migrated to Access Manager 11.1.2.

Sun Java System Access Manager 7.1 has two types of policies:

- **Referral Policies**: These policies do not apply to migration.
- **Non-Referral Policies**: These policies are migrated.

### Rules

- A Sun Java System Access Manager 7.1 policy without a rule is not supported for migration. Such policy is considered invalid.
- Rules that have the actions `GET` and `POST` are only applicable for migration. These rules have the service type as `URL Policy Agent`.
- Rules with other service types such as `Discovery Service` that has the actions `LOOKUP` and `UPDATE`, and service type `Liberty Personal Profile Service` that has the actions `QUERY` and `MODIFY` are not applicable for migration because these actions (which are known as resource operations in Access Manager 11.1.2) are not supported in Access Manager 11.1.2.

### Subjects

Only the subject type `AM Identity Subject` (user and group) and `Authenticated Users` are supported for migration. These subjects are migrated as part of **Identity Condition** in Access Manager 11.1.2.

### Conditions

- Active Session Time
  - This condition of Sun Java System Access Manager 7.1 policy is mapped to the attribute `Session Expiry Time` of the AttributeCondition in Access Manager 11.1.2.
  - The attribute `Terminate session` of this condition is ignored during migration as the appropriate mapping of this attribute does not exist in Access Manager 11.1.2.

- Authentication by Module Instance
  - This condition of Sun Java System Access Manager 7.1 policy is migrated to Access Manager 11.1.2 as AuthN scheme, and not as a condition.
  - Table 16–1 lists the authentication modules of Sun Java System Access Manager 7.1 that are migrated and mapped with the AuthN scheme into Access Manager 11.1.2.

***Table 16–1 Mapping of Authentication Module***

| Authentication Module in Sun Java System Access Manager 7.1 | Authentication Plug-in in Access Manager 11.1.2 |
|---|---|
| Certificate auth module | X509 auth plug-in |
| WindowsDesktopSSO auth module | Kerberos auth plug-in |
| LDAP auth module | LDAP auth plug-in |

- Authentication Level (less than or equal to) and Authentication Level (greater than or equal to)
  - Both the conditions of Sun Java System Access Manager 7.1 policy are mapped to the session attributes of the AttributeCondition with namespace SESSION and attribute name Authentication Level.
  - Both the conditions are mapped to the AttributeOperator EQUALS, as Access Manager 11.1.2 does not have corresponding mapping for greater then or equal to and less than or equal to. This mapping is done because of the equals factor in the policy condition in Sun Java System Access Manager 7.1. Therefore, both the conditions greater then or equal to and less than or equal to are similar in Access Manager 11.1.2.

    For example, if you migrate a Sun Java System Access Manager 7.1 policy with a condition of authentication level less than or equal to 5, the migrated policy in Access Manager 11.1.2 will have the authentication level equal to 5.
- Current Session Properties
  - This condition is mapped to the session attributes of the AttributeCondition with namespace SESSION and attribute name Other, where the key/value will be added as attributes of this condition. This condition in Sun Java System Access Manager 7.1 is multi-valued. Therefore, this condition in Access Manager 11.1.2 has multiple attributes with same name but different values.
- Identity Membership
  - This condition in Sun Java System Access Manager 7.1 policy is mapped to Identity condition in Access Manager 11.1.2.
  - All the unique users or groups from all the subjects, and all the unique users or groups from all the identity membership conditions in Sun Java System Access Manager 7.1 are created as a set of users or groups in one Identity condition in Access Manager 11.1.2.
  - During run-time verification, the ORing is performed between this set of users or groups
- IP Address/DNS Name
  - The condition IP Address in Sun Java System Access Manager 7.1 policy is mapped to IP condition in Access Manager 11.1.2.

  - The condition `DNS name` is not supported in Access Manager 11.1.2.

- LDAP Filter Condition
  - This condition in Sun Java System Access Manager 7.1 policy is mapped to `Identity condition` in Access Manager 11.1.2.
  - All the unique LDAP filters from all the LDAP filter conditions in Sun Java System Access Manager 7.1 are created as a set of LDAP filters in one Identity condition in Access Manager 11.1.2.
- Time (day, date, time, and time zone)
  - This condition in Sun Java System Access Manager 7.1 policy is mapped to `Time condition` in Access Manager 11.1.2.
  - The `Time` condition in Sun Java System Access Manager 7.1 contains one of the following values: date, time, day, or time zone; whereas the `Time` condition in Access Manager 11.1.2 contains either time or day. Therefore, the `Time` condition in Sun Java System Access Manager 7.1 containing only the time (start and end time) and day can be mapped to the `Time` condition in Access Manager 11.1.2. All the other cases are ignored.

#### Response Providers

- Sun Java System Access Manager 7.1 Server or Policy Server sends Identity or User repository attributes (that is, user attributes from any user store) to the agent as response providers. The OpenSSO agent sends these attributes back to the resource or application via Http header, request attribute, or Http cookie according to the configuration of the agent.

  All of the response providers (static as well as dynamic) are migrated from Sun Java System Access Manager 7.1 to Access Manager 11.1.2 with the type Http header.

### 16.3.3 Summary of Migration of User Stores

This section summarizes the migration of user stores from Sun Java System Access Manager 7.1 to Access Manager 11.1.2.

OpenSSO Enterprise has three types of user stores:

- **Active Directory**: This user store can be migrated to Access Manager 11.1.2.
- **Generic LDAPv3**: This user store can be migrated to Access Manager 11.1.2.
- **Sun DS with OpenSSO schema**: This user store cannot be migrated to Access Manager 11.1.2, as no supported data store type is available in 11.1.2.

### 16.3.4 Summary of Migration of Authentication Stores

This section summarizes the migration of authentication stores from Sun Java System Access Manager 7.1 to Access Manager 11.1.2.

The following are the authentication stores in Sun Java System Access Manager 7.1 that can be migrated and mapped to the corresponding authentication modules in Access Manager 11.1.2:

- LDAP in Sun Java System Access Manager 7.1 is mapped to OAM LDAP in Access Manager 11.1.2.
- Certificate in Sun Java System Access Manager 7.1 is mapped to X509 in Access Manager 11.1.2.

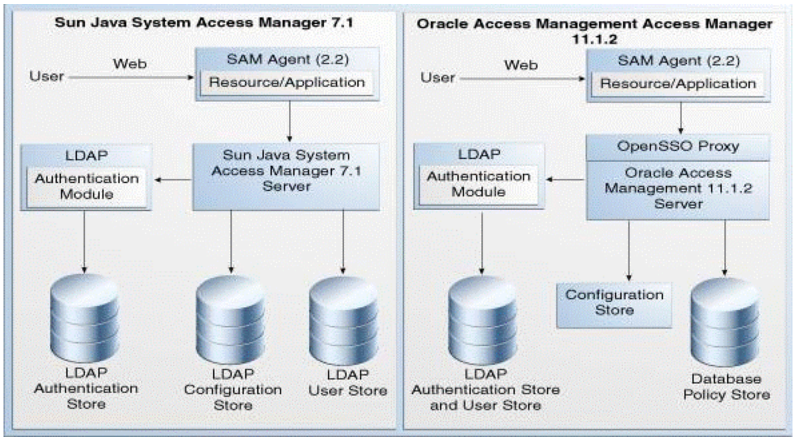
- Windows Desktop SSO in Sun Java System Access Manager 7.1 is mapped to Kerberos Access Manager 11.1.2.

All authentication stores with type LDAP are migrated to Access Manager 11.1.2 with name `AS_RealmName_Modulename`. The authentication stores with type other than LDAP are not migrated.

## 16.4 Topology Comparison

Figure 16–1 compares the topologies of Sun Java System Access Manager 7.1 and Access Manager 11.1.2.

***Figure 16–1 Sun Java System Access Manager 7.1 and Access Manager 11.1.2 Topologies***



## 16.5 Migration Roadmap

Table 16–2 lists the steps to migrate Sun Java System Access Manager 7.1 to Access Manager 11.1.2.

***Table 16–2 Task Roadmap***

| Task No | Task | For More Information |
|---|---|---|
| 1 | Complete the prerequisites. | See, Prerequisites for Migration |
| 2 | Install Oracle Identity and Access Management 11.1.2. | See, Installing Oracle Identity and Access Management 11.1.2 |
| 3 | Configure Oracle Access Management Access Manager 11.1.2. | See, Configuring Oracle Access Manager 11.1.2 |
| 4 | Generate the assessment report, and analyze what artifacts can be migrated to Access Manager 11.1.2.<br>You can perform this task multiple times. | See, Generating the Assessment Report |

*Table 16–2 (Cont.) Task Roadmap*

| Task No | Task | For More Information |
|---|---|---|
| 5 | Start the WebLogic Administration Server. | See, Starting the WebLogic Administration Server |
| 6 | Migrate Sun Java System Access Manager 7.1 to Access Manager 11.1.2 by running the migration tool. | See, Migrating the Artifacts of Sun Java System Access Manager 7.1 to OAM 11.1.2 |
| 7 | Complete the post-migration steps. | See, Post-Migration Tasks |
| 8 | Verify the migration. | See, Verifying the Migration |

## 16.6 Prerequisites for Migration

You must complete the following prerequisites for migrating Sun Java System Access Manager 7.1 to Access Manager 11.1.2:

1. Read the Oracle Fusion Middleware System Requirements and Specifications document to ensure that your environment meets the minimum requirements for the products you are installing, upgrading, and migrating.

   **Note:** For information about Oracle Fusion Middleware concepts and directory structure, see "Understanding Oracle Fusion Middleware Concepts and Directory Structure" in the *Oracle Fusion Middleware Installation Planning Guide for Oracle Identity and Access Management*.

2. Verify that the Sun Java System Access Manager version that you are using is supported for migration. For information about supported starting points for Sun Java System Access Manager 7.1 migration, see Section 11.6, "Supported Starting Points for Sun Java System Access Manager Migration".

## 16.7 Installing Oracle Identity and Access Management 11.1.2

As part of the migration process, you must freshly install Oracle Identity and Access Management 11.1.2 This 11.1.2 installation can be on the same machine where Sun Java System Access Manager 7.1 is installed, or on a different machine.

For more information about installing Oracle Identity and Access Management 11.1.2, see "Installing Oracle Identity and Access Management (11.1.2)" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

## 16.8 Configuring Oracle Access Manager 11.1.2

After you install Oracle Identity and Access Management 11.1.2, you must configure Access Manager 11.1.2 in a domain.

For more information about configuring Access Manager 11.1.2, see "Configuring Oracle Access Management" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

## 16.9 Generating the Assessment Report

This section describes how to generate an assessment report using the OpenSSO Agent assessment tool. This assessment report provides a preview of agents, policies, user stores, and authentication stores that are available in the Sun Java System Access Manager 7.1 deployment, and indicates which artifacts can be migrated to Access Manager 11.1.2.

You can generate an assessment report more than once before you can start the migration process.

This section includes the following topics:

- Obtaining the Tool
- Specifying LDAP Connection Details
- Updating the Agent Profile of 2.2 Agents
- Running the OpenSSO Agent Assessment Tool
- Analyzing the Assessment Report

> **Note:** Before you run the assessment tool, you must complete the following prerequisites:
>
> - Start the container on which Access Manager 7.1 is deployed.
> - Make sure that you use 1.6 or higher version of JDK.
> - Set the variable `JAVA_HOME` to the appropriate location where JDK 1.6 is installed.

### 16.9.1 Obtaining the Tool

Move from your present working directory to the location *`IAM_HOME`*`/oam/server/tools/opensso_assessment` using the following command:

**On UNIX**:

```
cd IAM_HOME/oam/server/tools/opensso_assessment/
```

**On Windows**:

```
cd IAM_HOME\oam\server\tools\opensso_assessment\
```

Extract the contents of the `OpenssoAgentdiscTool.zip` folder to a directory of your choice. It is recommended that you use the name `OpenssoAgentdiscTool` to the unzipped folder.

### 16.9.2 Specifying LDAP Connection Details

You must specify LDAP connection details in the properties file before you run the assessment tool by doing the following:

1. Open the `OpenSSOAgentDiscTool.properties` file from the following location:

   **On UNIX**: *`unzipped_folder`*`/resources/`

   **On Windows**: *`unzipped_folder`*`\resources\`

2. Set the appropriate values for the following properties:

   - `openSSOLDAPServerURL=`*`host`*`:`*`port`*

In this property, *host* and *port* refer to the LDAP host and the port of the configuration store used in Sun Java System Access Manager 7.1.

- `openSSOLDAPBindDN=`*`login_id`*

  where *login_id* is the bind DN of the LDAP server. You must have the administrative or root permissions to the configuration directory server of Sun Java System Access Manager 7.1.

- `openSSOLDAPSearchBase=`*`LDAP_search_base`*

  where *LDAP_search_base* is LDAP search base for the configuration store.

3. Save the file, and close.

> **Note:** If you do not specify the LDAP connection details, a message will be displayed in the `UserStoresInfo.txt` and `AuthnStoreInfo.txt` files. This message indicates that the information is not available. The same message will be displayed in the user stores and authentication stores sections in `DashBoardInfo.txt` file. You must then specify the right LDAP connection details in the `OpenSSOAgentDiscTool.properties` file, save the file, and run the assessment tool again.
>
> If you specify any incorrect value for any of these parameters, you cannot run the assessment tool, and error is displayed accordingly.

## 16.9.3 Updating the Agent Profile of 2.2 Agents

Before you run the OpenSSO Agent assessment tool, you must update the agent profiles of 2.2 agents that you wish to migrate, with the appropriate values for the attributes `agentRootURL` and `type` of the agent under **Agent Key Values(s)**. To do this, complete the following steps:

1. Log in to the Sun Java System Access Manager 7.1 administration console using the following URL:

   `http://`*`host`*`:`*`port`*`/amserver`

2. Go to the **Access Control** tab, and click the realm under which the 2.2 agent is installed.
3. Go to the **Subjects** tab, and click the **Agent** tab.
4. Click on the link for the agent to be migrated.
5. Under **Agent Key Value(s)**, if the values for the attributes `agentRootURL` and `Type` are not already present, enter these attributes with the appropriate values in the following format in the **New Value** field.

   `agentRootURL=`*`agent_webcontainer_URL`*

   `Type=WebAgent/J2EEAgent`

   Click **Add** after typing each attribute.
6. Click **Save**.

## 16.9.4 Running the OpenSSO Agent Assessment Tool

To run the OpenSSO Agent assessment tool, do the following:

1. Change your directory to the folder where you extracted the contents to, as described in Section 16.9.1, "Obtaining the Tool", using the following command:

   ```
   cd <path to the unzipped folder>
   ```

2. Run the following command:

   ```
   java -jar openssoagentdisc.jar <sam server URL> <username> <debugLevel>
   ```

   where

   `<sam server URL>` is the URL of the Sun Java System Access Manager 7.1 Server. You must specify it in the format: `http://<host>:<port>/amserver` where, `<host>` and `<port>` refer to hostname and port of the machine on which Sun Java System Access Manager 7.1 Server is running.

   `<username>` is the username of the Sun Java System Access Manager 7.1 Server

   `<debugLevel>` is optional. The value of this argument should be either `error` or `message`. If you do not specify this argument in the command, it takes the default value `error`.

   You are prompted to enter the following:

   1. `Enter server login password:`

      Enter the password of the Sun Java System Access Manager 7.1 server admin user. This user is typically the **amadmin**.

   2. `Enter LDAP login password:`

      Enter the login password of the LDAP server.

      **Note:** For more information about the arguments used in this command, run the following command in the unzipped directory:

      ```
      java -jar openssoagentdisc.jar -help
      ```

### 16.9.5 Analyzing the Assessment Report

The assessment tool generates five report files in the following location:

*unzipped_folder*/consoleOutput/

These reports contain the information about agents, policies, user stores, and authentication stores of Sun Java System Access Manager 7.1 that are supported in Access Manager 11.1.2.

Table 16–3 lists the report files that are generated when you run the assessment tool.

***Table 16–3 Report Files Generated***

| File | Description |
|---|---|
| `AgentInfo.txt` | Contains information about J2EE and web agents, and the list of supported agents in OAM 11*g*. |
| `AuthnStoreInfo.txt` | Contains information about authentication stores. |
| `DashBoardInfo.txt` | Contains brief information about agents, policies, user stores, and authentication stores. |

*Table 16–3 (Cont.) Report Files Generated*

| File | Description |
|---|---|
| `PolicyInfo.txt` | Contains information about policies. |
| `UserStoreInfo.txt` | Contains information about user stores. |

## 16.10 Starting the WebLogic Administration Server

You must start the WebLogic Administration Server before you can run the migration tool.

To start the Administration Server, do the following:

**On UNIX**:

1. Move from your present working directory to the `MW_HOME/user_projects/domains/domain_name/bin` directory using the command:

   ```
   cd MW_HOME/user_projects/domains/domain_name/bin/
   ```

2. Run the following command:

   ```
   startWebLogic.sh
   ```

   When prompted, enter the username and password of the WebLogic Administration Server.

**On Windows**:

1. Move from the present working directory to the`MW_HOME\user_projects\domains\domain_name\bin` directory using the following command on the command line:

   ```
   cd MW_HOME\user_projects\domains\domain_name\bin\
   ```

2. Run the following command:

   ```
   startWebLogic.cmd
   ```

   When prompted, enter the username and password of the WebLogic Administration Server.

## 16.11 Migrating the Artifacts of Sun Java System Access Manager 7.1 to OAM 11.1.2

Before you start the actual migration of the artifacts from Sun Java System Access Manager 7.1 to Access Manager 11.1.2, make sure that you have generated the assessment report (as described in Section 16.9, "Generating the Assessment Report"), and analyzed what artifacts can be migrated to Access Manager 11.1.2.

To migrate Sun Java System Access Manager 7.1 to Access Manager 11.1.2, do the following:

1. Create a properties file at any accessible location. For example, create the `oam_migration.properties` file.

   Enter values for the following properties in the properties file:

   - `openSSOServerURL=<sam server URL>`
   - `openSSOAdminUser=<sam admin username>`

- `openSSOAdminPassword=`
- `openSSOServerDebugLevel=error/message`
- `openSSOLDAPServerURL=<LDAP host:port>`
- `openSSOLDAPBindDN=<LDAP bind DN>`
- `openSSOLDAPBindPwd=`
- `openSSOLDAPSearchBase=<LDAP searchBase>`

Table 16–4 describes the values you must specify for each of the properties in the properties file.

***Table 16–4 Property File Values***

| Property | Description |
|---|---|
| `openSSOServerURL` | Specify the URL of the Sun Java System Access Manager 7.1 Server. It must be specified in the format:<br>`http://<host>:<port>/amserver`<br>where<br>`<host>` is the machine on which the Sun Java System Access Manager 7.1 Administration Server is running<br>`<port>` is the port number of the Sun Java System Access Manager 7.1 Administration Server |
| `openSSOAdminUser` | Specify the username of the Sun Java System Access Manager 7.1 Administration Server. |
| `openSSOAdminPassword` | Do not specify any value for this property. The migration tool prompts you for the Sun Java System Access Manager 7.1 admin password when you run the migration command, as described in step-4. |
| `openSSOServerDebugLevel` | Specify one of the following values:<br>■ `error`<br>■ `message`<br>This value represents the debug level. |
| `openSSOLDAPServerURL` | Specify the URL of the LDAP server. This must be specified in the format:<br>*`host`*`:`*`port`*<br>where,<br>`host>` refers to the LDAP host of the configuration store used in Sun Java System Access Manager 7.1<br>`<port>` refers to the LDAP port of the configuration store used in Sun Java System Access Manager 7.1 |
| `openSSOLDAPBindDN` | Specify the bind DN of the LDAP server. This user must have the admin or root permissions to the configuration directory server of Sun Java System Access Manager 7.1. |
| `openSSOLDAPBindPwd` | Do not specify any value for this property. The migration tool prompts you for the LDAP bind password when you run the migration command as described in step-4. |
| `openSSOLDAPSearchBase` | Specify the LDAP search base for the configuration store. |

> **Note:** Do not specify any value for `openSSOAdminPassword` and `openSSOLDAPBindPwd` properties.

2. Run the following command to launch the WebLogic Scripting Tool (WLST):

   **On UNIX**:

   a. Move from your present working directory to the *IAM_HOME*/common/bin directory by running the following command on the command line:

   ```
   cd IAM_HOME/common/bin
   ```

   b. Run the following command to launch the WebLogic Scripting Tool (WLST):

   ```
   ./wlst.sh
   ```

   **On Windows**:

   a. Move from your present working directory to the *IAM_HOME*\common\bin directory by running the following command on the command line:

   ```
   cd IAM_HOME\common\bin
   ```

   b. Run the following command to launch the WebLogic Scripting Tool (WLST):

   ```
   wlst.cmd
   ```

3. Run the following command to connect WLST to the WebLogic Server instance:

   ```
   connect('wls_admin_username','wls_admin_password','t3://hostname:port');
   ```

   In this command,

   *wls_admin_username* is the username of the WebLogic Administration Server.

   *wls_admin_password* is the password of the WebLogic Administration Server.

   *hostname* is the machine where WebLogic Administration Server ia running.

   *port* is the Administration Server port

4. Run the following command to migrate the artifacts of Sun Java System Access Manager 7.1 to Access Manager 11.1.2:

   ```
   oamMigrate(oamMigrateType="OpenSSO",pathMigrationPropertiesFile="<absolute_
   path_of_properties_file>");
   ```

   where

   `<absolute_path_of_properties_file>` is the absolute path to the properties file that you created in step-1. For example:

   **On UNIX**:
   ```
   oamMigrate(oamMigrateType="OpenSSO",pathMigrationPropertiesFile="abc/de
   f/oam_migration.properties"
   ```

   **On Windows**:
   ```
   oamMigrate(oamMigrateType="OpenSSO",pathMigrationPropertiesFile="abc\\d
   ef\\oam_migration.properties
   ```

   You are prompted to enter the following:

   1. `Enter value for property : openSSOAdminPassword :`

      Enter the password of the Sun Java System Access Manager 7.1 Administration Server.

2. `Enter value for property : openSSOLDAPBindPwd :`

   Enter the bind password of the LDAP server.

> **Note:** Complete migration is performed when you run `oamMigrate()` command for the first time.
>
> After an initial migration (complete migration), you can re-execute this command to perform a delta migration.
>
> For more information about complete and delta migration, see Section 16.2, "Modes of Migration".

When the migration is complete, the WLST console displays a message stating the result of the migration.

## 16.12 Post-Migration Tasks

After you migrate Sun Java System Access Manager 7.1 to Access Manager 11.1.2, you must complete the following post-migration tasks:

1. This migration tool creates the `AMAgent.properties` file at the following location:

   ```
   <domain_home>/<domain_name>/output/OpenSSOMigration/AM7.1/<realm_
   name>/<agent_name>/AMAgent.properties
   ```

   You must replace the `@DEBUG_LOGS_DIR@` tag in the `AMAgent.properties` file with the valid directory path to the debug logs on the agent host. To do this, complete the following steps:

   a. Open the `AMAgent.properties` file.

   b. In the property `com.sun.am.policy.agents.config.local.log.file =@DEBUG_LOGS_DIR@/amAgent`, replace the tag `@DEBUG_LOGS_DIR@` with the valid directory path to the debug logs on the agent host.

2. You must back up the existing properties file, which is on the agent host, and copy the newly created `AMAgent.properties` file to the agent host. To do this, complete the following steps:

   a. Stop the agent web container instance.

   b. Back up the existing properties file (that is the properties file which existed on the agent host before you started the migration process).

   c. Copy the newly created `AMAgent.properties` file from the following location to the agent host:

      ```
      <domain_home>/<domain_name>/output/OpenSSOMigration/AM7.1/<realm_
      name>/<agent_name>/AMAgent.properties
      ```

   d. Start the agent web container instance.

   After you do this, any access to a protected resource will redirect the user to the Access Manager 11.1.2 server for authentication.

3. The migration tool does not retrieve the passwords of the user stores that are migrated from Sun Java System Access Manager 7.1 to Access Manager 11.1.2. Therefore, after migration, you must manually update the passwords for all the user stores that are migrated. To do this, complete the following steps:

   a. Log in to the Oracle Access Management 11.1.2 console using the following URL:

      ```
      http://host:port/oamconsole
      ```

      where *host* is the machine on which Access Manager 11.1.2 is running, and *port* is the port number.

   b. Go to the **System Configuration** tab.

   c. Expand **Data Sources** under **Common Configuration** on the left navigation pane.

   d. Expand **User Identity Stores**, manually update the password for all the migrated LDAP user stores that exist.

4. After migration, the minimum and maximum pool size for the migrated authentication stores will be set to 0, by default. Hence, you must manually set the appropriate values for **Minimum Pool Size** and **Maximum Pool Size** for the authentication stores in the Oracle Access Management 11.1.2 console. To do this, complete the following steps:

   a. Log in to the Oracle Access Management 11.1.2 console using the URL:

      ```
      http://host:port/oamconsole
      ```

   b. Go to the **System Configuration** tab.

   c. Expand **Common Configuration** on the left navigation pane.

   d. Expand **Data Sources**, and then expand **User Identity Stores**.

   e. Select the authentication store to be edited.

   f. Scroll down to **Connection Details**, and set the values **Minimum Pool Size** and **Maximum Pool Size**. For example, Minimum Pool Size=10 and Maximum Pool Size=50.

   g. Click **Apply**.

## 16.13 Verifying the Migration

To verify the migration, do the following:

1. Log in to the Oracle Access Management 11.1.2 console using the following URL:

   ```
   http://host:port/oamconsole
   ```

   In this URL,

   - *host* refers to fully qualified domain name of the machine hosting the Oracle Access Management 11.1.2 console.
   - *port* refers to the designated bind port for the Oracle Access Management 11.1.2 console, which is the same as the bind port for the Administration Server.

   Verify that the Sun Java System Access Manager 7.1 agents (2.2 agents), user stores, authentication stores, authentication modules, host identifiers, resources, policies with correct authentication scheme having correct authentication module are migrated to Access Manager 11.1.2.

2. Access any protected page using the URL. The URL now redirects you to the Oracle Access Management 11.1.2 Server login page. Upon successful

authentication, it should perform a successful authorization and you should be able to access the resource successfully.

# 17

# Coexistence of Oracle Access Manager 10*g* with Oracle Access Management Access Manager 11.1.2

This chapter describes how to setup an environment where both Oracle Access Manager 10*g* and Oracle Access Management Access Manager (Access Manager) 11*g* Release 2 (11.1.2) deployments coexist, after you migrate from Oracle Access Manager 10*g* to Oracle Access Management Access Manager 11.1.2. In this coexistence scenario, the Oracle Access Manager 10*g* Server does the authentication for all the resources.

This chapter contains the following sections:

## 17.1 Coexistence Overview

During the process of migration from Oracle Access Manager 10*g* to Access Manager 11.1.2, you can have both Oracle Access Manager 10*g* and Access Manager 11.1.2 deployments coexisting, so that some applications are protected by Oracle Access Manager 10*g* while others are protected by Access Manager 11.1.2. It is desirable for end-users to have a seamless single sign-on experience when they navigate between these applications. This is called the coexistence mode.

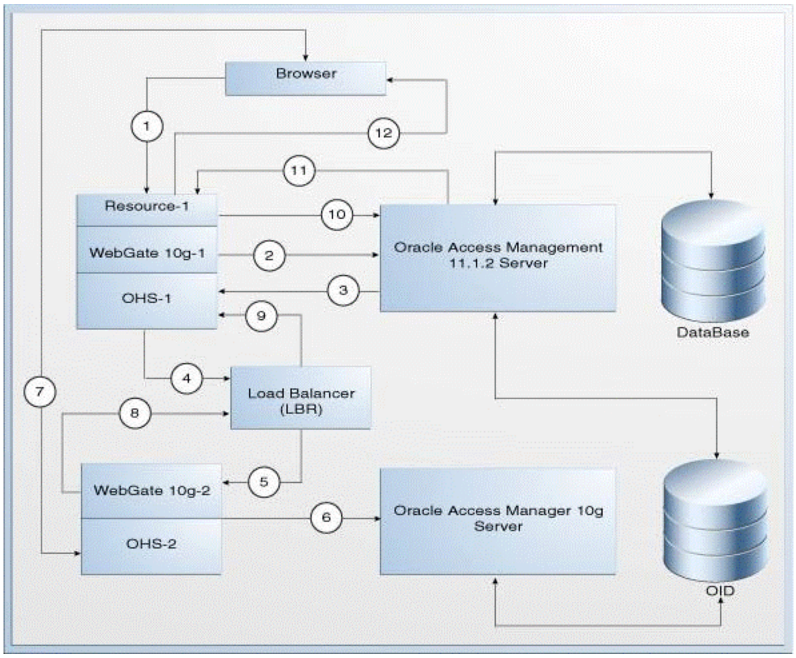
In this mode, Access Manager 11.1.2 protects the migrated applications and any new applications registered with Access Manager 11.1.2; whereas Oracle Access Manager 10*g* continues to protect the applications that are not migrated to Access Manager 11.1.2.

In this coexistence mode, Oracle Access Manager 10*g* performs the authentication for all the resources protected by Access Manager 11.1.2.

## 17.2 Coexistence Topology

Figure 17–1 illustrates how the Oracle Access Manager 10*g* Server coexists with the Access Manager 11.1.2 Server.

***Figure 17–1 Coexistence of Oracle Access Manager 10g with Access Manager 11.1.2***



The topology consists of disjoint Oracle Access Manager 10*g* and Access Manager 11.1.2 setups. The numbers 1-12 in the topology show the sequence in which the requests flow in the coexistence environment. Table 17–1 describes the request flow.

This coexistence setup contains the following:

- Oracle Access Manager 10*g* WebGate partners registered against Access Manager 11.1.2 Server.
- Oracle Access Manager 10*g* WebGate partners registered against Oracle Access Manager 10*g* Server.

### Topology Description

- `WebGate 10g-1`: This refers to the 10*g* or 11*g* WebGate partner registered with Access Manager 11.1.2 Server. It is deployed on Oracle HTTP Server 11*g* named `OHS-1`. `WebGate 10g-1` protects the resources or applications that are migrated to Access Manager 11.1.2.
- `WebGate 10g-2`: This refers to the Oracle Access Manager 10*g* WebGate partner registered with Oracle Access Manager 10*g* Server. It is deployed on Oracle HTTP

Server 11*g* named OHS-2. WebGate 10*g*-2 protects the resources or applications that are not migrated to Access Manager 11.1.2, and are supposed to be protected by Oracle Access Manager 10*g*. It also protects the credential collector URLs.

- OHS-1: This refers to the Oracle HTTP Server 11*g* on which WebGate 10*g*-1 is deployed.
- OHS-2: This refers to the Oracle HTTP Server 11*g* on which WebGate 10*g*-2 is deployed. OHS-2 acts as a reverse proxy for Access Manager 11.1.2 Managed Server's host and port. It front-ends the credential collector of Access Manager 11.1.2. For this reason, you must use the OHS module for WebLogic.
- Resource-1: This is any resource protected by Access Manager 11.1.2 Server.
- Load Balancer (LBR): This is a logical load balancer that maps to the configuration in Access Manager 11.1.2.

Table 17–1 describes the request flow. The numbers in the **Step** column correspond to the numbers shown in the topology in Figure 17–1.

***Table 17–1 Request Flow***

| Step | Description |
|---|---|
| 1 | User requests access to Resource-1, which is protected by Access Manager 11.1.2 Server at the following URL:<br>http://OHS-1:port/Resource1<br>where OHS-1 is the hostname of the Oracle HTTP Server 11*g* (OHS-1), and the port is the port number of the machine on which OHS-1 is running. |
| 2 and 3 | WebGate 10*g*-1 which is deployed on OHS-1 intercepts the request, and communicate with the Access Manager 11.1.2 server to obtain the Access Manager 11.1.2 Server authentication end point. |
| 4 and 5 | WebGate 10*g*-1 redirects to the authentication end point of Access Manager 11.1.2 Server. This goes to the OHS-2 (WebGate 10*g*-2), as OHS-2 acts as reverse proxy for the Access Manager 11.1.2 server's credential collector. |
| 6 | WebGate 10*g*-2 is registered against the Oracle Access Manager 10*g* Server, and Access Manager 11.1.2 Server authentication end point URL itself is protected by Oracle Access Manager 10*g* with desired authentication scheme such as form authentication scheme. Therefore, WebGate 10*g*-2 redirects the user to a login form to collect the credentials. |
| 7 | When the user provides the credentials, WebGate10*g*-2 communicates with Oracle Access Manager 10*g* Server to perform authentication followed by authorization. After authorization, the Oracle Access Manager 10*g* server provides all relevant headers (**OAM_REMOTE_USER**) and cookies to WebGate10*g*-2 according to the policy configuration, and these are then set by the WebGate. |
| 8, 9, and 10 | Once WebGate 10*g*-2 successfully authenticates and authorizes access to the Access Manager 11.1.2 Server authentication end point, the request to Access Manager 11.1.2 Server authentication end point passes to the Access Manager 11.1.2 Managed Server port. |
| 11 | The Access Manager 11.1.2 server asserts (using header **OAM_REMOTE_USER**) as Resource-1 is protected at Access Manager 11.1.2 server using the **OAM10gScheme**. All relevant headers and cookies are set and redirected to Resource-1. |

## 17.3 Task Roadmap

Table 17–2 lists the steps to set up and configure the topology shown in Figure 17–1.

*Table 17–2 Tasks to be Completed*

| Task No | Task | For More Information |
|---|---|---|
| 1 | Understand and get familiar with the coexistence topology before you start the configuration process. | See, Coexistence Topology |
| 2 | Complete the prerequisites. | See, Prerequisites for Coexistence |
| 3 | Install two new Oracle HTTP Server 11*g* instances (`OHS-1` and `OHS-2`), or two different Oracle HTTP Server installations.<br>If you do not wish to install two new Oracle HTTP Server instances, you can use the Oracle HTTP Server instance, which is available as part of your Oracle Access Manager 10*g* migration. | See, Optional: Installing and Configuring Oracle HTTP Server 11g (OHS-1 and OHS-2) |
| 4 | Configure `OHS-2` as a reverse proxy for Access Manager 11.1.2 Managed Server. | See, Configuring OHS-2 as a Reverse Proxy for Access Manager 11.1.2 Managed Server |
| 5 | Update the authentication module **LDAPNoPasswordAuthModule** in Access Manager 11.1.2, and point the User Identity Store to the data source that is created in Access Manager 11.1.2 as a result of migration. | See, Updating LDAPNoPasswordAuthModule in Access Manager 11.1.2 |
| 6 | Install two WebGates: `WebGate 10g-1` and `WebGate 10g-2`.<br>`WebGate 10g-1` should be deployed on `OHS-1`, and configured with Access Manager 11.1.2 Server. This WebGate can be a 10*g* or and 11*g* WebGate.<br>`WebGate 10g-2` should be deployed on `OHS-2`, and configured with Oracle Access Manager 10*g* Server. This WebGate must be a 10*g* WebGate.<br>If you do not wish to install new WebGates, you can use the WebGates that are available as part of your Oracle Access Manager 10*g* migration. | See, Optional: Installing and Configuring WebGate 10g-1 and WebGate 10g-2 |
| 7 | Configure separate primary cookie domains for each of the WebGates. | See, Configuring Separate Primary Cookie Domains for two WebGate Instances |
| 8 | Protect all the resources at Access Manager 11.1.2. | See, Protecting Resources at Access Manager 11.1.2 |

*Table 17–2 (Cont.) Tasks to be Completed*

| Task No | Task | For More Information |
|---|---|---|
| 9 | Protect the Access Manager 11.1.2 authentication end point URL in Oracle Access Manager 10*g*. | See, Protecting the Authentication End Point URL of Access Manager 11.1.2 in Oracle Access Manager 10g |
| 10 | Configure the logout settings to make sure that the logout works at both the WebGates and the Access Manager 11.1.2 server. | See, Configuring Logout Settings |
| 11 | Configure the session management. | See, Configuring Session Management Settings |
| 12 | Verify the configuration. | See, Verifying the Configuration |

## 17.4 Prerequisites for Coexistence

You must complete the following prerequisites before you start performing tasks required for coexistence of Oracle Access Manager 10*g* with Access Manager 11.1.2.

1. Read the Oracle Fusion Middleware System Requirements and Specifications document to ensure that your environment meets the minimum requirements for the products you are installing, upgrading, and migrating.

> **Note:** For information about Oracle Fusion Middleware concepts and directory structure, see "Understanding Oracle Fusion Middleware Concepts and Directory Structure" in the *Oracle Fusion Middleware Installation Planning Guide for Oracle Identity and Access Management*.

2. Verify that the version of Oracle Access Manager 10*g* that you are using is supported for coexistence. For more information about supported starting points for coexistence of Oracle Access Manager 10*g* with Access Manager 11.1.2, see Section 11.7, "Supported Starting Points for Coexistence of Oracle Access Manager 10g With Oracle Access Management Access Manager 11.1.2".
3. Migrate the artifacts of Oracle Access Manager 10*g* to Access Manager 11.1.2. For more information, see Chapter 12, "Migrating Oracle Access Manager 10g Environments".
4. Make sure that Oracle Access Manager 10*g* and Access Manager 11.1.2 share the same user store.
5. Make sure that the Oracle Access Manager 10*g* and the Oracle Access Management 11.1.2 servers are up and running.

## 17.5 Optional: Installing and Configuring Oracle HTTP Server 11*g* (OHS-1 and OHS-2)

Install and configure Oracle HTTP Server 11*g* (`OHS-1` and `OHS-2`, as shown in Figure 17–1). Alternatively, you can use the Oracle HTTP Server instances that exist after migration from Oracle Access Manager 10*g* to Access Manager 11.1.2.

For more information, see "Installing and Configuring Oracle HTTP Server 11*g*" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

## 17.6 Configuring OHS-2 as a Reverse Proxy for Access Manager 11.1.2 Managed Server

You must configure `OHS-2` as a reverse proxy for Access Manager 11.1.2 server, so that it front ends the Access Manager 11.1.2 Server authentication end point, which is the Access Manager 11*g* Managed Server's host and port.

> **Note:** As mentioned earlier, `OHS-2` can be either an existing OHS installation on which `WebGate 10`*g* is installed and configured with Oracle Access Manager 10*g* or a new OHS installation.

To configure OHS-2 as a reverse proxy for Access Manager 11.1.2 server, do the following:

1. Set up `OHS-2` to forward requests with the URL prefix "`/oam`" to the Access Manager 11.1.2 Server, by configuring `mod_wl_ohs`, the OHS plug-in for Oracle WebLogic Server

   For more information about configuring OHS module for WebLogic, see "Configuring the mod_wl_ohs Module" in *Oracle Fusion Middleware Administrator's Guide for Oracle HTTP Server*.

   While configuring `mod_wl_ohs`, the `WebLogicHost` and `WebLogicPort` parameters should point to the host and port of the appropriate Access Manager 11.1.2 Server.

2. Restart `OHS-2`.

3. Log in to the Oracle Access Management 11.1.2 console using the following URL:

   ```
   http://host:port/oamconsole
   ```

   In this URL,

   *`host`* refers to the fully qualified domain name of the machine hosting the Oracle Access Management 11.1.2 console (Administration Server)

   *`port`* refers to the designated bind port for the Oracle Access Management 11.1.2 console, which is the same as the bind port for the Administration Server

   `/oamconsole` refers to the Oracle Access Manager console login page

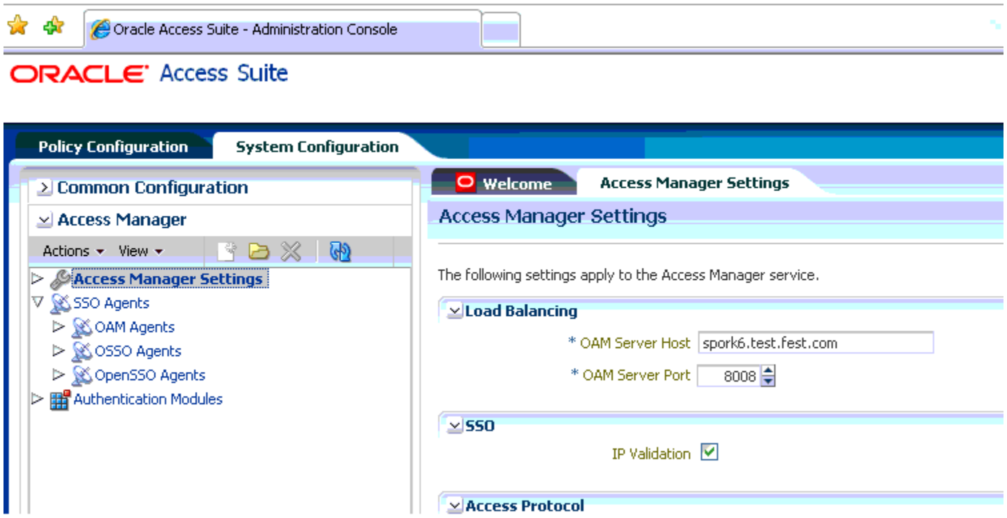
4. Go to the **System Configuration** tab, and then double-click on **Access Manager Settings**.

5. In the section **Load Balancing**, specify the hostname of `OHS-2` in the **OAM Server Host** field, and the port number of `OHS-2` in the **OAM Server Port** field.

6. Click **Apply**.

   Figure 17–2 shows the Access Manager 11.1.2 console where you must change the Access Manager Settings.

*Figure 17–2 Changing the Load Balancing Settings*



Access Manager Settings

The following settings apply to the Access Manager service.

Load Balancing

* OAM Server Host spork6.test.fest.com

* OAM Server Port 8008

SSO

IP Validation ☑

Access Protocol

7. To use the IP validation feature of `WebGate 10g-1`, which is configured with Access Manager 11.1.2 Server, you must make changes to the Access Manager 11.1.2 Server, so that the Access Manager 11.1.2 Server uses the IP address of the client to create an SSO token. To do this, complete the following steps:

   a. Log in to the WebLogic Administration console using the following URL:

   `http://host:port/console`

   where,

   *`host`* is the hostname of the machine on which WebLogic is running

   *`port`* is the port number of the machine on which WebLogic is running

   b. Expand **Environments** under **Domain Structure** in the left navigation pane.

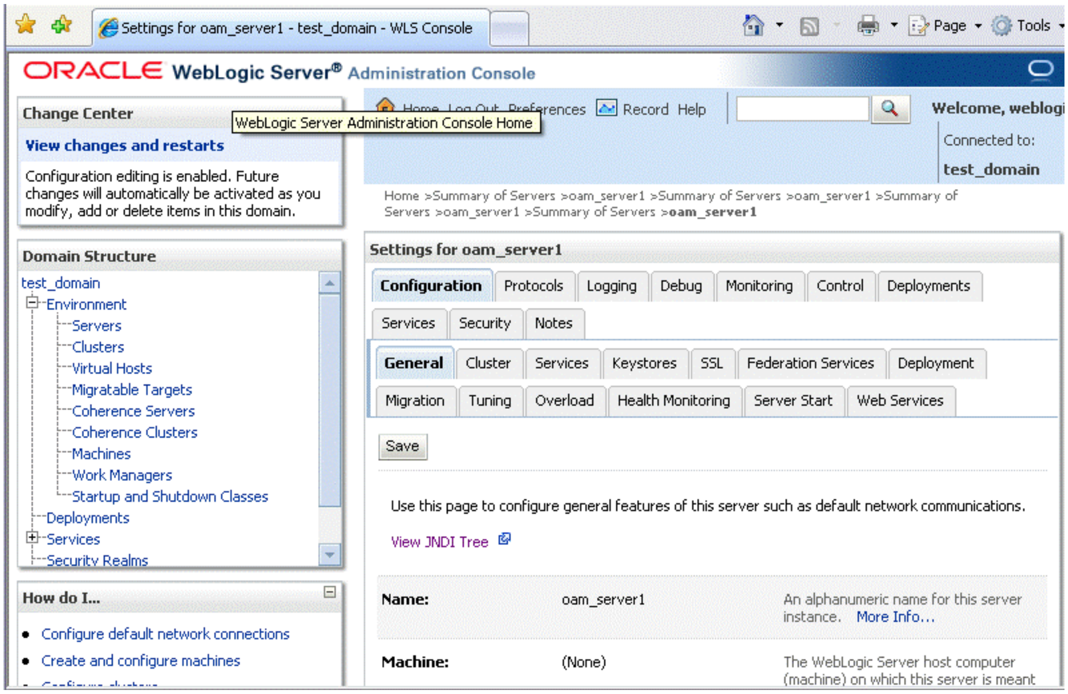
   c. Select **Servers**.

   d. Select **OAM Server** from **Summary of Servers** in the right panel.

   e. Select the **Configuration** tab, and then click the **General** tab.

   Figure 17–3 shows the tabs that you must select in WebLogic console.

*Figure 17–3 Selecting the OAM Server*



Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

Home >Summary of Servers >oam_server1 >Summary of Servers >oam_server1 >Summary of Servers >oam_server1 >Summary of Servers >**oam_server1**

Use this page to configure general features of this server such as default network communications.

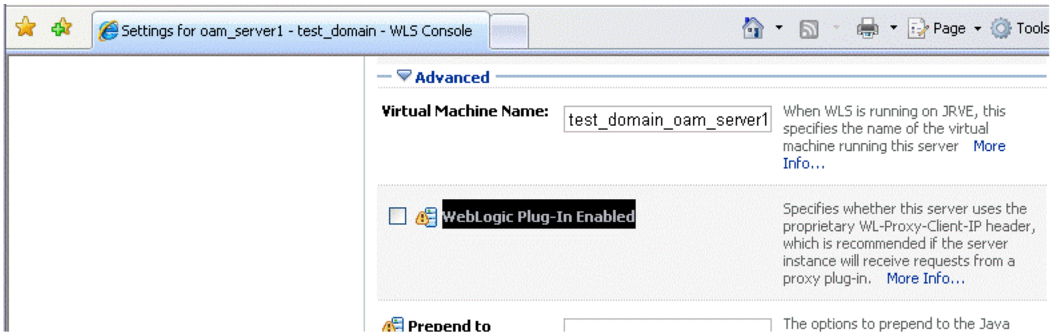
**Name:** oam_server1 — An alphanumeric name for this server instance. More Info...

**Machine:** (None) — The WebLogic Server host computer (machine) on which this server is meant

f. Click **Advanced**, and then select the **WebLogic Plug-In Enabled** option.

Figure 17–4 shows the checkbox that you must select.

*Figure 17–4 Selecting WebLogic Plug-In Enabled*



**Virtual Machine Name:** test_domain_oam_server1 — When WLS is running on JRVE, this specifies the name of the virtual machine running this server More Info...

□ **WebLogic Plug-In Enabled** — Specifies whether this server uses the proprietary WL-Proxy-Client-IP header, which is recommended if the server instance will receive requests from a proxy plug-in. More Info...

**Prepend to** — The options to prepend to the Java

g. Click **Save**.

h. Restart the WebLogic Administration Server and the Access Manager 11.1.2 Managed Servers by completing the following tasks:

a. Stop the WebLogic Administration Server.

b. Stop the Access Manager Managed Servers.

c. Start the WebLogic Administration Server.

d. Start the Access Manager Managed Servers.

For more information about starting and stopping the servers, see "Starting and Stopping Administration Servers" and "Starting and Stopping Managed Servers" in the *Oracle Fusion Middleware Administrator's Guide*.

## 17.7 Updating LDAPNoPasswordAuthModule in Access Manager 11.1.2

**LDAPNoPasswordAuthModule** is the authentication module used by the authentication scheme - **OAM10gScheme**.

You must update the authentication module **LDAPNoPasswordAuthModule** to point to the data source that is created in Access Manager 11.1.2 as a result of migration. To do this, complete the following steps:

1. Log in to the Oracle Access Management 11.1.2 console using the following URL:

   ```
   http://host:port/oamconsole
   ```

   In this URL,

   - *host* refers to fully qualified domain name of the machine hosting the Oracle Access Manager console (Administration Server).
   - *port* refers to the designated bind port for the Oracle Access Management 11.1.2 console, which is the same as the bind port for the Administration Server.

2. Go to the **System Configuration** tab.
3. Expand **Access Manager**, and then expand **Authentication Modules**.
4. Expand **LDAP Authentication Module**.
5. Click **LDAPNoPasswordAuthModule**, and update the User Identity Stores to point to the data source that is created in Access Manager 11.1.2 as a result of migration.

## 17.8 Optional: Installing and Configuring WebGate 10*g*-1 and WebGate 10*g*-2

After the Oracle Access Manager 10*g* migration, you will have the old WebGate which communicates with the Oracle Access Manager 10*g* Server (`WebGate 10g-2`), and the migrated WebGate, which communicates with the Access Manager 11.1.2 Server (WebGate 10*g*-1). You can either use these two WebGate instances for setting up the coexistence environment, or install two new WebGate instances.

If you wish to install new WebGates instances: `WebGates 10g-1` and `WebGates 10g-2`, you must configure them as follows:

- `WebGate 10g-1`: This WebGate instance can be Oracle Access Manager 10*g* WebGate or Access Manager 11.1.2 WebGate. You must install a 10*g* or 11*g* WebGate on Oracle HTTP Server 11*g* (`OHS-1`), as shown in Figure 17–1, and configure it with the Access Manager 11.1.2 Server.

  For information on installing 10*g* WebGate, and configuring it with the Access Manager 11.1.2 server, see "Locating and Installing the Latest 10*g* Webgate for Oracle Access Manager 11*g*" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.

  For information on installing 11*g* WebGate, and configuring it with the Access Manager 11.1.2 server, see "Installing and Configuring Oracle HTTP Server 11*g* Webgate for OAM" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

- `WebGate 10g-2`: This is a 10*g* WebGate instance that acts as a proxy for WebLogic. You must install 10*g* WebGate on Oracle HTTP Server 11*g* (`OHS-2`), as shown in Figure 17–1, and configure it with the Oracle Access Manager 10*g* Server.

For information on installing 10*g* WebGate, and configuring it with the Oracle Access Manager 10*g* Server, see "Installing the WebGate" in the *Oracle Access Manager Installation Guide* for release 10*g* (10.1.4.3).

> **Note:** For more information about managing 10*g* WebGates with Access Manager 11.1.2, see "Managing 10*g* Webgates with Oracle Access Manager 11*g*" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.

## 17.9 Configuring Separate Primary Cookie Domains for two WebGate Instances

If the resource WebGate (`WebGate 10g-1`) configured with the Access Manager 11.1.2 Server is of type 10*g* WebGate, you must create separate primary cookie domains for each of the WebGate instances (`WebGate 10g-1` and `WebGate 10g-2`). To do this, complete the following steps:

1. Create different primary cookie domain for each of the WebGates. You can do this by modifying the profiles of both the WebGate instances.

   To modify the profile of `WebGate 10g-1` that is configured with the Access Manager 11.1.2 server, do the following:

   a. Log in to the Oracle Access Management 11.1.2 console using the following URL:

   ```
   http://host:port/oamconsole
   ```

   b. Go to the **System Configuration** tab.

   c. Click **Access Manager**, and then click **SSO Agents**.

   d. Double-click **OAM Agents**.

   e. Search for the WebGate for which profile needs to be modified, by typing the WebGate ID in the Search panel to the right of the console window. Click the pencil icon to edit the profile.

   f. Change the value of the parameter **Primary Cookie Domain**, and click **Apply**.

2. Similarly, modify the profile of `WebGate 10g-2` that is configured with Oracle Access Manager 10*g* Server, and specify the appropriate value for the parameter **Primary HTTP cookie Domain**. For more information, see "Modifying an AccessGate" in the *Oracle Access Manager Access Administration Guide* for release 10*g* (10.1.4.3).

3. Use virtual hosting to get different domains for the two WebGates on OHS. For more information, see "Configuring Virtual Hosts by Editing the HTTP Server Configuration Files" in the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management*.

   Since you are using virtual hosting to create different domains for the WebGates, you must make some configuration changes to the WebGate. For more information about configuring virtual hosting for the WebGates, see "Configuring Virtual Web Hosting" in the *Oracle Access Manager Access Administration Guide* for release 10*g* (10.1.4.3).

## 17.10 Protecting Resources at Access Manager 11.1.2

Resource `WebGate 10g-1`, which is configured with the Access Manager 11.1.2 Server has to protect the resources with the special authentication scheme (**OAM10gScheme**).

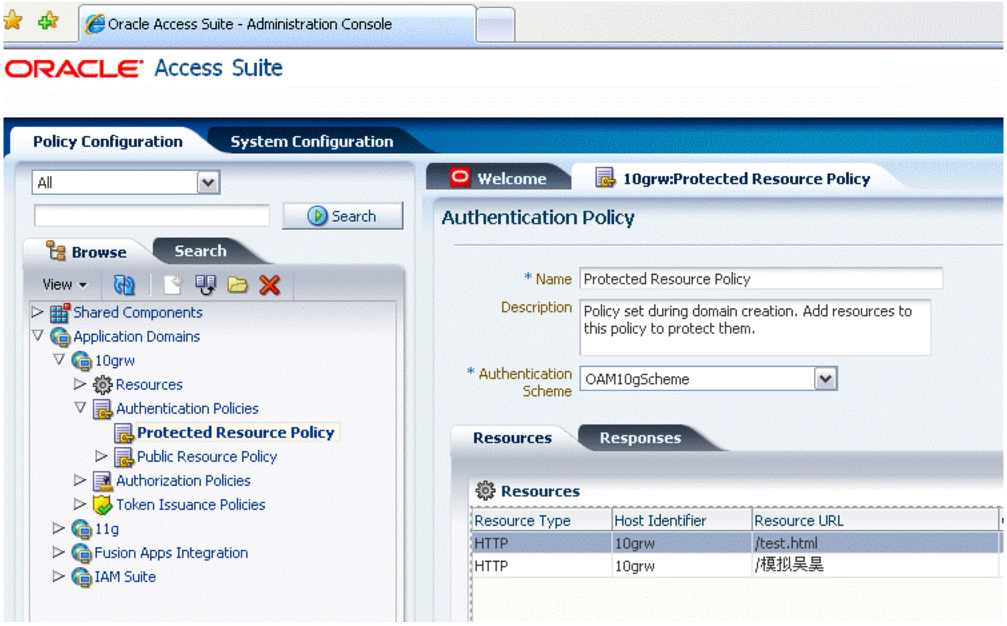
To achieve this, you must either change the authentication scheme of the existing authentication policy, or you must have a new application domain and create a new policy.

For information about making changes to the authentication scheme of the existing policy, see "Viewing or Editing an Authentication Policy" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.

For information about creating and managing policies, see "Managing Policies to Protect Resources and Enable SSO" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.

Figure 17–5 shows the authentication scheme that you must select for the authentication policy which protects the resources.

***Figure 17–5 Protected Policy with Authentication Scheme***



Authentication Policy

* Name: Protected Resource Policy

Description: Policy set during domain creation. Add resources to this policy to protect them.

* Authentication Scheme: OAM10gScheme

Resources

| Resource Type | Host Identifier | Resource URL |
|---|---|---|
| HTTP | 10grw | /test.html |
| HTTP | 10grw | /模拟吴昊 |

This illustration shows the authentication scheme that you must select for the authentication policy that protects the resources.

********************************************************************************************************************

## 17.11 Protecting the Authentication End Point URL of Access Manager 11.1.2 in Oracle Access Manager 10*g*

In this coexistence environment, `WebGate 10g-2` that is configured with Oracle Access Manager 10*g* Server, and the associated Oracle Access Manager 10*g* server performs authentication on behalf of Access Manager 11.1.2 by protecting the authentication end point URL of Access Manager 11.1.2.

The following resource must be protected by an Oracle Access Manager 10*g* policy:

**/oam/server/obrareq.cgi**

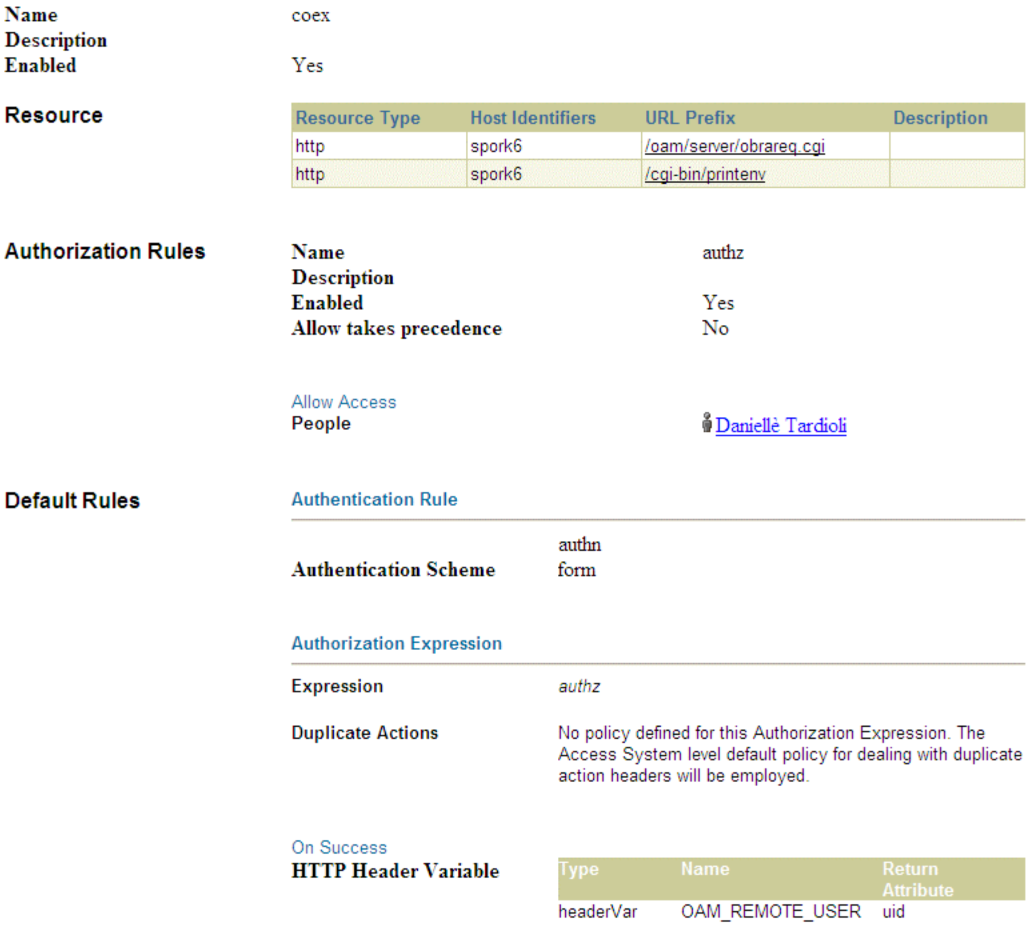
To protect this resource, create an Oracle Access Manager 10*g* policy and do the following:

- Specify the desired authentication scheme
- Specify the list of users who are authorized to access the resource **/oam/server/obrareq.cgi**
- Configure **OAM_REMOTE_USER** as the HTTP header success action in the authorization expression. You must set the value of the user ID to this header.

For more information about creating policies, see "Protecting Resources with Policy Domains" in the *Oracle Access Manager Access Administration Guide* for release 10*g* (10.1.4.3).

Figure 17–6 shows a sample policy domain.

***Figure 17–6 Sample Policy Domain***



| | |
|---|---|
| **Name** | coex |
| **Description** | |
| **Enabled** | Yes |

**Resource**

| Resource Type | Host Identifiers | URL Prefix | Description |
|---|---|---|---|
| http | spork6 | /oam/server/obrareq.cgi | |
| http | spork6 | /cgi-bin/printenv | |

**Authorization Rules**

| | |
|---|---|
| **Name** | authz |
| **Description** | |
| **Enabled** | Yes |
| **Allow takes precedence** | No |

Allow Access

| | |
|---|---|
| **People** | Danièllè Tardioli |

**Default Rules**

Authentication Rule

| | |
|---|---|
| | authn |
| **Authentication Scheme** | form |

Authorization Expression

| | |
|---|---|
| **Expression** | *authz* |
| **Duplicate Actions** | No policy defined for this Authorization Expression. The Access System level default policy for dealing with duplicate action headers will be employed. |

On Success

**HTTP Header Variable**

| Type | Name | Return Attribute |
|---|---|---|
| headerVar | OAM_REMOTE_USER | uid |

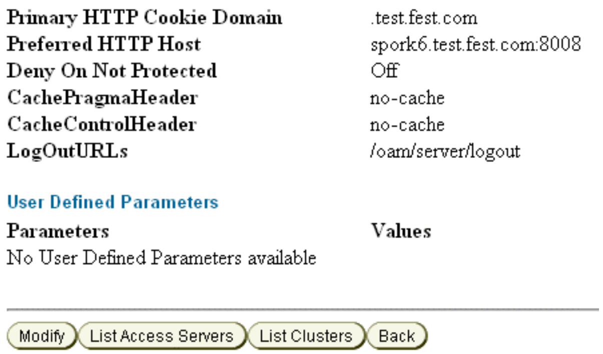
## 17.12 Configuring Logout Settings

You must configure the logout settings, and make sure that logout works at both the WebGates and the Access Manager 11.1.2 Server. To do this, complete the following steps:

1. Modify the profile of `WebGate 10g-2`, and set the value of **LogOutURLs**. This value must be the same as that of the logout end point URL of Access Manager 11.1.2 Server, that is **/oam/server/logout**. For more information, see "Modifying an AccessGate" in the *Oracle Access Manager Access Administration Guide* for release 10*g* (10.1.4.3).

   Figure 17–7 shows a sample profile of `WebGate 10g-2`.

***Figure 17–7 Sample WebGate 10g-2 Profile***



| | |
|---|---|
| **Primary HTTP Cookie Domain** | .test.fest.com |
| **Preferred HTTP Host** | spork6.test.fest.com:8008 |
| **Deny On Not Protected** | Off |
| **CachePragmaHeader** | no-cache |
| **CacheControlHeader** | no-cache |
| **LogOutURLs** | /oam/server/logout |

User Defined Parameters

| **Parameters** | **Values** |
|---|---|
| No User Defined Parameters available | |

2. Perform the following steps to configure logout, depending on the type of `WebGate 10g-1` that is configured with the Access Manager 11.1.2 Server.

   **If the resource WebGate (WebGate 10*g*-1) is a 11*g* WebGate:**

   Make sure that the **Logout Redirect URL** parameter is set to the URL pointing to the host and port of `OHS-2`, as shown in the following example:

   ```
   http://OHS-2_host:OHS-2_port/oam/server/logout
   ```

   In this URL,

   *`OHS-2_host`* is the host on which `OHS-2` is running.

   *`OHS-port`* is the port of `OHS-2`.

   To do this, complete the following steps:

   a. Log in to the Oracle Access Management 11.1.2 console using the following URL:

      ```
      http://host:port/oamconsole
      ```

   b. Go to the **System Configuration** tab.

   c. Click **Access Manager**, and then click **SSO Agents**.

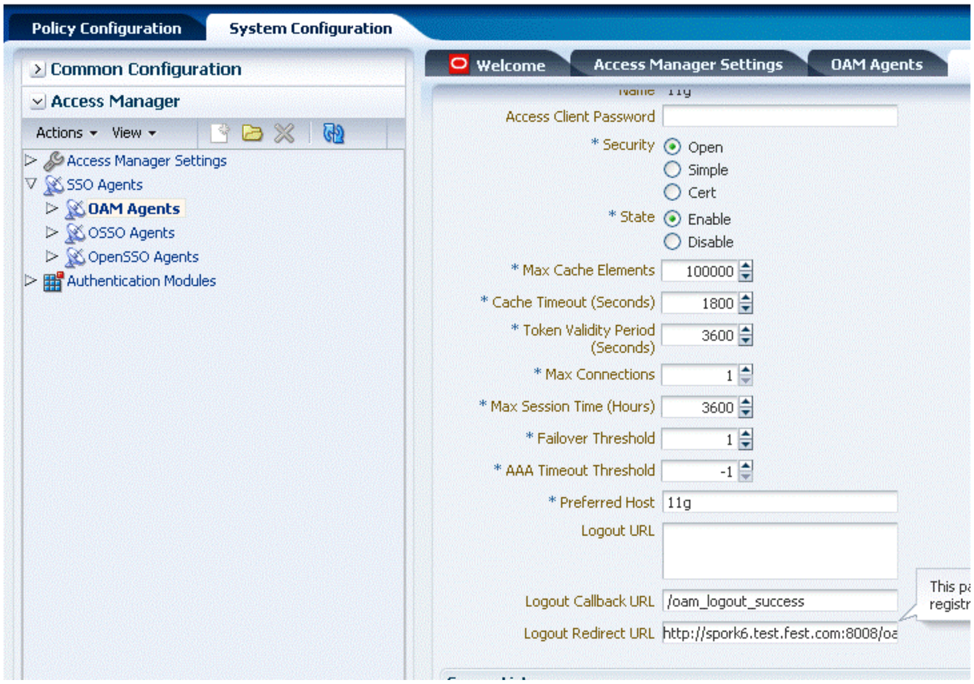
   d. Double-click **OAM Agents**.

   e. Search for the WebGate for which profile needs to be modified, by typing the WebGate ID in the Search panel to the right of the console window. Click the pencil icon to edit the profile.

   f. Change the value of the parameter **Logout Redirect URL**, and click **Apply**.

   Figure 17–8 shows the WebGate profile where you must specify the **Logout Redirect URL**.

*Figure 17–8 WebGate Logout Redirect URL Configuration*



Name 11g

Access Client Password

* Security ● Open ○ Simple ○ Cert

* State ● Enable ○ Disable

* Max Cache Elements 100000

* Cache Timeout (Seconds) 1800

* Token Validity Period (Seconds) 3600

* Max Connections 1

* Max Session Time (Hours) 3600

* Failover Threshold 1

* AAA Timeout Threshold -1

* Preferred Host 11g

Logout URL

Logout Callback URL /oam_logout_success

Logout Redirect URL http://spork6.test.fest.com:8008/oa

**g.** Use the following URL to initiate and verify logout from the resource WebGate (`WebGate 10g-1`):

```
http://OHS-1_host:OHS-1_port/logout.html
```

In this URL,

*`OHS-1_host`* is the host on which `OHS-1` is running.

*`OHS-1_port`* is the port of `OHS-1`.

As this URL is directed to `logout.html`, `WebGate 10g-1` clears the SSO cookie, and redirects to the **Logout Redirect URL** that you specified in step-1. Since the host and port of `OHS-2` is used for the **Logout Redirect URL**, this request comes to `WebGate 10g-2` which is deployed on `OHS-2`. The logout URL for `WebGate 10g-2` is **/oam/server/logout**, and the `WebGate 10g-2` clears SSO cookie, and forwards the request to the Access Manager 11.1.2 Server. The Access Manager 11.1.2 Server finally clears all the sessions.

**h.** Use the following URL to initiate and verify logout from the authentication WebGate (`WebGate 10g-2`):

```
http://OHS-2_host:OHS-2_port/oam/server/logout
```

In this URL,

*`OHS-2_host`* is the host on which `OHS-2` is running.

*`OHS-2_port`* is the port of `OHS-2`.

As the logout URL for `WebGate 10g-2` is **/oam/server/logout**, WebGate 10*g*-2 clears the SSO cookie, and forwards the request to the Access Manager 11.1.2 server. Access Manager 11.1.2 Server now clears the session, and calls the Logout Callback URL of `WebGate 10g-1`. This makes the `WebGate 10g-1` to clear its own SSO cookie.

**If the resource WebGate (WebGate 10*g*-1) is a 10*g* WebGate:**

a. Modify the `logout.html` file which is generated when you register `WebGate 10g-1` with the Access Manager 11.1.2 Server. Set the variable `SERVER_LOGOUTURL` in the `logout.html` file to the logout URL, which points to the host and port of `OHS-2` as shown in the following example:

```
var SERVER_LOGOUTURL="http://OHS-2_host:OHS-2_port/oam/server/logout
```

   In this URL,

   *`OHS-2_host`* is the host on which `OHS-2` is running.

   *`OHS-2_port`* is the port of `OHS-2`.

b. Use the following URL to initiate and verify logout from the resource WebGate (`WebGate 10g-1`):

```
http://OHS-1_host:OHS-1_port/logout.html
```

   In this URL,

   *`OHS-1_host`* is the host on which `OHS-1` is running.

   *`OHS-1_port`* is the port of `OHS-1`.

   This clears the SSO cookie at `WebGate 10g-1`, and `WebGate 10g-1` redirects to the **Logout Redirect URL**, which, in turn, directs to `OHS-2` because the **Logout Redirect URL** points to the host and port of `OHS-2`. The request comes to WebGate 10*g*-2 which is deployed on `OHS-2`. The logout URL for `WebGate 10g-2` is **/oam/server/logout**. Therefore, `WebGate 10g-2` clears the SSO cookie, and forwards the request to the Access Manager 11.1.2 server. The Access Manager 11.1.2 server finally clears all the sessions.

c. To initiate logout from the authentication WebGate (`WebGate 10g-2`), add the `end_url` parameter pointing to the full logout URL of the resource WebGate (`WebGate 10g-1`) as a query string to the logout URL, as shown in the following example:

```
http://OHS-2_host:OHS-2_port/oam/server/logout?end_url=http://OHS-1_
host:OHS-1_port/logout.html
```

   In this URL,

   *`OHS-2_host`* is the host on which `OHS-2` is running.

   *`OHS-2 port`* is the port of `OHS-2`.

   *`OHS-1_host`* is the host on which `OHS-1` is running.

   *`OHS-1_port`* is the port of `OHS-1`.

   This clears the SSO cookie at the authentication WebGate (`WebGate 10g-2`), and `WebGate 10g-2` forwards the request to the Access Manager 11.1.2 Server. The Access Manager 11.1.2 Server now clears the session, and redirects it to the local logout URL of the resource WebGate (`WebGate 10g-1`) as we have specified the `end_url` parameter. The resource WebGate (`WebGate 10g-1`) clears its own SSO cookie.

3. Optional: If you wish to allow users to access the logout URL, configure a policy in Oracle Access Manager 10*g*. For information about creating an Oracle Access Manager 10*g* policy, see "Protecting Resources with Policy Domains" in the *Oracle Access Manager Access Administration Guide* for release 10*g* (10.1.4.3).

## 17.13 Configuring Session Management Settings

When a user accesses a resource on the resource WebGate (`WebGate 10g-1`), a separate session is established with the Access Manager 11.1.2 server, after the Oracle Access Manager 10*g* Server authenticates the user. On session timeout or idle session timeout for the session with the Access Manager 11.1.2 Server, the user is redirected to the authentication WebGate (`WebGate 10g-2`). On `WebGate 10g-2`, the user is prompted for re-authentication on session timeout or the idle session timeout of the Oracle Access Manager 10*g* Server session.

As a result, session timeouts are derived from the 10*g* WebGate configured with 10*g* server (10*g*-2).

For 10*g* or 11g WebGate (`WebGate 10g-1`) that is configured with Access Manager 11.1.2 server, the parameters that affect the session management are `Session Lifetime` and `Idle Timeout`. To view or edit these parameters, do the following:

1. Log in to the Oracle Access Management 11.1.2 console using the following URL:

   ```
   http://host:port/oamconsole
   ```

2. Go to the **System Configuration** tab, and click **Common Configuration**.
3. Select **Common Settings**.

For 10*g* WebGate (`WebGate 10g-2`) that is configured with Oracle Access Manager 10*g* server, the parameters that affect session management are `Maximum user session time` and `Idle Session Time`, which are part of the WebGate profile. You can change the values of these parameters by modifying the profile of `WebGate 10g-2`. For more information, see "Modifying an AccessGate" in the *Oracle Access Manager Access Administration Guide* for release 10*g* (10.1.4.3).

You must ensure that the sessions of both the WebGates are synchronized. For this, make sure that the values specified for the parameters **Maximum user session time** and **Idle Session Time** of `WebGate 10g-2` are equal to or less than the values specified for the corresponding parameters of `WebGate 10g-1`: **Session Lifetime** and **Idle Timeout**.

**Note:** For more information about session management of the Access Manager 11.1.2 Server, see "Managing Sessions" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.

## 17.14 Verifying the Configuration

You must verify the configuration by doing the following:

1. After you access the protected resource on `WebGate 10g-1`, observe the HTTP header and verify that it redirects to `WebGate 10g-2`, that is, the host and port of `OHS-2`. If the redirection occurs, you are prompted to provide credentials for authentication according to the authentication scheme used to protect **/oam/server/obrareq.cgi**.
2. Verify that the resource that you requested in step-1 is displayed in the browser. Also, verify whether the SSO token is set for the configured domain at `WebGate 10g-1` and `WebGate 10g-2`.
3. Initiate logout from the same browser, and verify whether the SSO cookies are unset or set to `loggedout` at both the WebGates.

# 18

# Coexistence of Sun OpenSSO Enterprise 8.0 with Oracle Access Management Access Manager 11.1.2

This chapter describes how to set up an environment where both Sun OpenSSO Enterprise 8.0 (OpenSSO Enterprise) and Oracle Access Management Access Manager (Access Manager) 11*g* Release 2 (11.1.2) deployments coexist, after you migrate Sun OpenSSO Enterprise 8.0 to Oracle Access Management Access Manager 11.1.2.

This chapter contains the following sections:

## 18.1 Coexistence Overview

During the process of migration from OpenSSO Enterprise 8.0 to Oracle Access Manager 11.1.2.0.0, you can have both OpenSSO Enterprise 8.0 and Access Manager 11.1.2 deployments coexisting, such that some applications are protected by OpenSSO Enterprise 8.0 while others are protected by Access Manager 11.1.2. It is desirable for end-users to have a seamless single sign-on experience when they navigate between these applications. This is called coexistence mode.

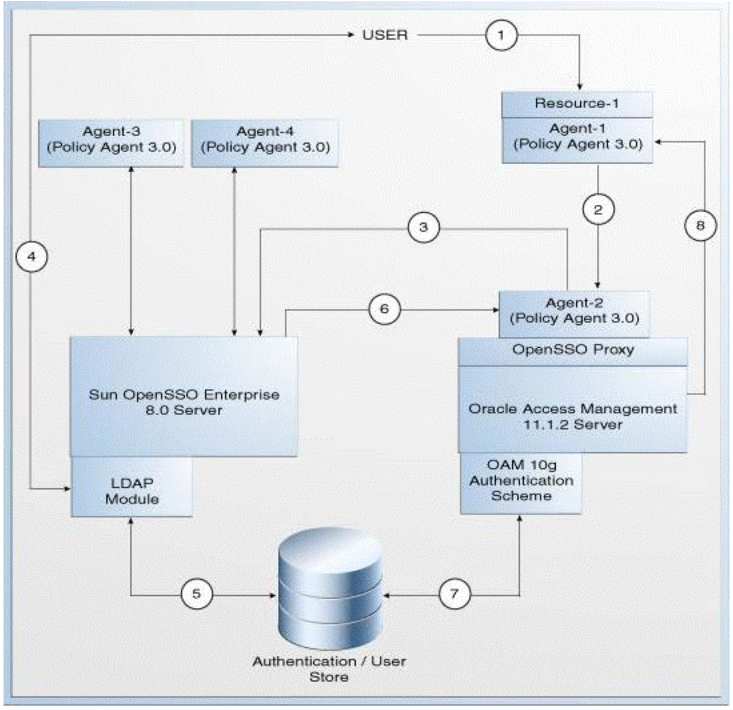
In this mode, Access Manager 11.1.2 protects the migrated applications and any new applications registered with Access Manager 11*g*; whereas OpenSSO Enterprise 8.0 continues to protect the applications that are not migrated to Access Manager 11.1.2.

In this coexistence mode, OpenSSO Enterprise 8.0 performs the authentication for all the resources protected by Access Manager 11.1.2.

## 18.2 Coexistence Topology

Figure 18–1 illustrates how the authentication is done by the OpenSSO Enterprise 8.0 server when a user requests to access a protected resource.

***Figure 18–1 Coexistence of OpenSSO Enterprise 8.0 with Access Manager 11.1.2***


USER
1
Resource-1
Agent-1 (Policy Agent 3.0)
Agent-3 (Policy Agent 3.0)
Agent-4 (Policy Agent 3.0)
2
3
8
4
6
Agent-2 (Policy Agent 3.0)
OpenSSO Proxy
Sun OpenSSO Enterprise 8.0 Server
Oracle Access Management 11.1.2 Server
LDAP Module
OAM 10g Authentication Scheme
5
7
Authentication / User Store

The topology consists of disjoint OpenSSO Enterprise 8.0 and Access Manager 11.1.2 environments. The numbers 1-8 in the topology show the sequence in which a request flows in the coexistence environment. See Table 18–2 for the request flow.

### Topology Description

- `Agent-1`: This is an OpenSSO agent (Policy Agent 3.0) registered with Access Manager 11.1.2 Server. It protects `Resource-1`.
- `Agent-2`: This is an OpenSSO agent (Policy Agent 3.0) registered with OpenSSO Enterprise 8.0 Server, which protects the end point URL of the Access Manager 11.1.2 server. This agent must be configured in the OpenSSO Enterprise 8.0 server. You must create a profile for this agent in OpenSSO Enterprise 8.0 Server, and freshly install a new Policy Agent (3.0).
- `Agent-3` and `Agent-4`: These are the OpenSSO Agents (Policy Agents 3.0) registered with the OpenSSO Enterprise 8.0 Server.
- `Resource-1`: This is a resource which is protected by `Agent-1` which communicates with the Access Manager 11.1.2 Server.
- `Policy-1`: This is the authentication policy created on the Access Manager 11.1.2 Server for protecting `Resource-1`. This policy is created as part of the task: Creating an Authentication Policy in Access Manager 11.1.2 to Protect Resource-1.

- `Policy-2`: This is the authentication policy created on OpenSSO Enterprise 8.0 server for Access Manager's opensso proxy endpoints protected by `Agent-2`. This policy is created as part of the task: Protecting the End-Point URL of Access Manager 11.1.2 Server Using Agent-2.

Table 18–2 describes the request flow. The numbers in the **Step** column correspond to the numbers in Figure 18–1.

***Table 18–1 Request Flow***

| Step | Description |
|---|---|
| 1 | User requests to access `Resource-1` which is protected by `Agent-1` that communicates with the Access Manager 11.1.2 Server. |
| 2 | `Agent-1` redirects the user to the Access Manager 11.1.2 Server for authentication (….`/opensso/UI/Login.....?goto=resource1`) using the authentication scheme **OAM10gAuthScheme** as per `Policy-1`. The user authenticated by OpenSSO Enterprise server is set in the **OAM_REMOTE_USER** header by the OpenSSO agent. Hence, `Agent-1` uses the authentication scheme **OAM10*g*AuthScheme** to assert the user from header **OAM_REMOTE_USER**. |
| 3 | The Access Manager 11.1.2 server end point is protected by `Agent-2` that communicates with the OpenSSO Enterprise 8.0 Server.<br>Therefore, `Agent-2` redirects the user to OpenSSO Enterprise 8.0 Server for LDAP authentication (`...opensso/UI/Login?goto=<`….*`/oam/server/.....?goto=resource1`*`>`) as per `Policy-2`. |
| 4 | The OpenSSO Enterprise 8.0 Server's LDAP authentication module prompts the user for LDAP user name and password. User must enter the valid LDAP credentials. |
| 5 | The OpenSSO Enterprise 8.0 Server validates the user credentials against authentication store, and creates user session as OpenSSO Enterprise 8.0 session and sets the OpenSSO Enterprise 8.0 SSO **cookie1** with this session ID. |
| 6 | The OpenSSO Enterprise 8.0 Server redirects the user to the Access Manager 11.1.2 Server (….`/opensso/UI/Login/.....?goto=resource1`). |
| 7 | `Agent-2` verifies the user session and policy evaluation by ensuring the presence of OpenSSO session **cookie1**. It now provides access to Access Manager 11.1.2 Server (….`/opensso/UI/Login/.....?goto=resource1)` after setting the header **OAM_REMOTE_USER** to the **userID** in **Session Attribute Mapping**.<br>The Access Manager 11.1.2 Server invokes the authentication scheme (**OAM10gAuthScheme**) as per step 2 (`Policy-1`), and asserts the user using the header **OAM_REMOTE_USER**, using the **OAM10gScheme** configured for the `Resource-1`. |
| 8 | The Access Manager 11.1.2 server creates the Access Manager session and sets headers. It also sets **OAM_ID** cookie and OpenSSO SSO **cookie2** (via OpenSSO Proxy) and redirects the user to `Resource-1`. OpenSSO Enterprise 8.0 SSO **cookie2** has link to related the **OAM_ID** cookie.<br>The user can now access `Resource-1`, as `Agent-1` verifies the user session and policy evaluation by ensuring the presence of OpenSSO session **cookie2** and **OAM_ID** cookie. |

## 18.3 Task Roadmap

Table 18–2 lists the steps to configure the coexistence environment.

*Table 18–2 Tasks to be Completed*

| Task No | Task | For More Information |
|---|---|---|
| 1 | Understand and get familiar with the coexistence topology before you start the configuration process. | See, Coexistence Topology |
| 2 | Complete the prerequisites. | See, Prerequisites for Coexistence |
| 3 | Create `Agent-2` profile on OpenSSO Enterprise 8.0 Server, and install `Agent-2`. Update the web applications `ngsso-web.war` and `openssoproxy-urlmapper.war` in `oam-server.ear` file.<br>Also, create an authentication policy on OpenSSO Enterprise 8.0 to protect the end point URL of the Access Manager 11.1.2 Server using `Agent-2`. | See, Protecting the End-Point URL of Access Manager 11.1.2 Server Using Agent-2 |
| 4 | Configure the data sources for Access Manager 11.1.2. | See, Configuring Data Source for Access Manager 11.1.2 |
| 5 | Update the authentication module in Access Manager 11.1.2, and point the user identity store to the data source that is configured in Section 18.6. | See, Updating LDAPNoPasswordAuthModule in Access Manager 11.1.2 |
| 6 | Create the profile of `Agent-1` in Access Manager 11.1.2, and install a new Policy Agent 3.0 (Agent-1) pointing to Access Manager 11.1.2 server. | See, Creating the Profile of Agent-1 in Access Manager 11.1.2 |
| 7 | Create an authentication policy in Access Manager 11.1.2 server to protect `Resource-1`. | See, Creating an Authentication Policy in Access Manager 11.1.2 to Protect Resource-1 |
| 8 | Change the default cookie name of Access Manager 11.1.2, so that the cookie names of Access Manager 11.1.2 and OpenSSO Enterprise 8.0 are different. | See, Modifying the OpenSSO Cookie Name in Access Manager 11.1.2 |

*Table 18–2 (Cont.) Tasks to be Completed*

| Task No | Task | For More Information |
|---|---|---|
| 9 | Update the profile of `Agent-2` in the OpenSSO Enterprise 8.0 Server with the right Session Attributes Mapping. | See, Updating the Profile of Agent-2 in OpenSSO Enterprise 8.0 Server |
| 10 | Configure logout setting to initiate logout from both OpenSSO Enterprise 8.0 server and Access Manager 11.1.2 Server. | See, Configuring Logout Settings |
| 11 | Verify the configuration. | See, Verifying the Configuration |

## 18.4 Prerequisites for Coexistence

Complete the following prerequisites before you start performing the tasks described in this chapter:

- Read the Oracle Fusion Middleware System Requirements and Specifications document to ensure that your environment meets the minimum requirements for the products you are installing, upgrading, and migrating.

> **Note:** For information about Oracle Fusion Middleware concepts and directory structure, see "Understanding Oracle Fusion Middleware Concepts and Directory Structure" in the *Oracle Fusion Middleware Installation Planning Guide for Oracle Identity and Access Management*.

- Verify that the version of OpenSSO Enterprise that you are using is supported for coexistence. For more information about supported starting points for OpenSSO Enterprise 8.0 coexistence, see Section 11.8, "Supported Starting Points for Coexistence of Sun OpenSSO Enterprise With Oracle Access Management Access Manager 11.1.2".
- Ensure that the Sun OpenSSO Enterprise 8.0 and Oracle Access Management Access Manager 11*g* Release 2 (11.1.2) installations are complete, and the servers are running.

  If you have not installed and configured Oracle Access Management Access Manager 11*g* Release 2 (11.1.2), you must do it before you start with the next task. For more information on installing and configuring Oracle Access Management Access Manager 11*g* Release 2 (11.1.2), see "Installing Oracle Identity and Access Management (11.1.2.0.0)" and "Configuring Oracle Access Management" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.
- Ensure that the OpenSSO Enterprise 8.0 and Access Manager 11.1.2 share the same user store.
- If OpenSSO Enterprise 8.0 and Access Manager 11.1.2 servers are running on different machines, make sure the time of these machines are synchronized.

## 18.5 Protecting the End-Point URL of Access Manager 11.1.2 Server Using Agent-2

You must create a profile for `Agent-2` in OpenSSO Enterprise 8.0, and freshly install a policy agent 3.0 to protect the end-point URL of the Access Manager 11.1.2 server. Also, you must create a policy for protecting the end-point URL of the Access Manager 11.1.2 Server in OpenSSO Enterprise 8.0 Server. To do this, complete the following tasks:

1. Creating Agent-2 Profile for Access Manager 11.1.2 on OpenSSO Enterprise 8.0 Server
2. Installing Agent-2 (Policy Agent 3.0)
3. Updating Web Applications to Include Agent Filter Configurations
4. Creating Authentication Policy on OpenSSO Enterprise 8.0 Server for Access Manager 11.1.2

### 18.5.1 Creating Agent-2 Profile for Access Manager 11.1.2 on OpenSSO Enterprise 8.0 Server

Create `Agent-2` profile (as shown in Figure 18–1) on the OpenSSO Enterprise 8.0 Server by doing the following:

1. Log in to the OpenSSO Enterprise 8.0 Server administration console using the URL:

   ```
   http://host:port/opensso
   ```

   In this URL,

   - *`host`* refers to the fully qualified domain name of the machine hosting the OpenSSO Enterprise 8.0 console
   - *`port`* refers to the designated bind port for the OpenSSO Enterprise 8.0 console, which is the same as the bind port for the Administration Server
2. Go to the **Access Control** tab.
3. Click the top realm under **Realm Name** column in **Realms** table.
4. Click **Agents** tab.
5. Click the **Web/J2EE** tab according to the type of agent that you wish to create and configure in the OpenSSO Enterprise 8.0 Server.
6. Click **New** to create the new `Agent-2`, and provide the necessary information such as **Name**, **Password**, **Configuration**, **Server URL**, and **Agent URL**.
7. Click **Create**.

### 18.5.2 Installing Agent-2 (Policy Agent 3.0)

Install `Agent-2` (Policy Agent 3.0) in front of the Access Manager 11.1.2 server. This should be a J2EE agent for WebLogic.

For more information about installing Policy Agent 3.0, see the respective sections in the *Sun OpenSSO Enterprise Policy Agent 3.0 Guide for Oracle WebLogic Server/Portal 10*

### 18.5.3 Updating Web Applications to Include Agent Filter Configurations

You must update the web applications `ngsso-web.war` and `openssoproxy-urlapper.war` to include the agent filter configurations in the `web.xml` file for Access Manager 11.1.2 Server to be protected by `Agent-2`. To do this, complete the following steps:

1. Unzip the `oam-server.ear` file from the *IAM_HOME*`/oam/server/apps/oam-server.ear` directory, and extract the contents to a temporary directory.
2. Extract the contents of the `ngsso-web.war` file, and then extract the contents of `web.xml` file. Update the `web.xml` file with the appropriate agent filter configuration for the Access Manager 11.1.2 Server to be protected by `Agent-2`. Update the filter definition with the URL: `/server/opensso/login/*` in `url-pattern`.

   For example:

   ```
   <filter>
   <filter-name>Agent</filter-name>
   <filter-class>com.sun.identity.agents.filter.AmAgentFilter</filter-class>
   </filter>
   <filter-mapping>
   <filter-name>Agent</filter-name>
   <url-pattern>/server/opensso/login/*</url-pattern>
   </filter-mapping>
   ```

3. Extract the contents of the `openssoproxy-urlmapper.war` file at the same location *IAM_HOME*`/oam/server/apps/oam-server.ear`. Update the `web.xml` file with the appropriate agent filter configuration for the Access Manager 11.1.2 server to be protected by `Agent-2`. Update the filter definition with the URL `/UI/*` in `url-pattern`.

   For example:

   ```
   <filter>
   <filter-name>Agent</filter-name>
   <filter-class>com.sun.identity.agents.filter.AmAgentFilter</filter-class>
   </filter>
   <filter-mapping>
   <filter-name>Agent</filter-name>
   <url-pattern>/UI/*</url-pattern>
   </filter-mapping>
   ```

4. Re-package the `oam-server.ear` file to include the updated `ngsso-web.war` and `openssoproxy-urlapper.war` files.
5. Redeploy the updated `oam-server.ear` file.

### 18.5.4 Creating Authentication Policy on OpenSSO Enterprise 8.0 Server for Access Manager 11.1.2

You must create an authentication policy (referred to as `Policy-1`) on OpenSSO Enterprise 8.0 Server to protect the end point URL of the Access Manager 11.1.2 Server. To do this, complete the following steps:

1. Log in to the OpenSSO Enterprise 8.0 Server administration console using the URL:

   http://*host*:*port*/opensso

In this URL,

- *host* refers to the fully qualified domain name of the machine hosting the OpenSSO Enterprise 8.0 console (Administration Server)
- *port* refers to the designated bind port for the OpenSSO Enterprise 8.0 console, which is the same as the bind port for the Administration Server

2. Go to the **Access Control** tab.
3. Click the top realm under **Realm Name** column in **Realms** table.
4. Click the **Policies** tab.
5. Click **New Policy**, and provide the details of the new policy for protecting the end point URL of Access Manager 11.1.2 server with **Rule** as `OAM_server_protocol://OAM_managed_server_host:OAM_managed_server_port/opensso/UI/Login*?*` and `OAM_server_protocol://OAM_managed_server_host:OAM_managed_server_port/oam/server/opensso/login*`, and **Subject** as **Authenticated Users**.
6. Click **OK**.

## 18.6 Configuring Data Source for Access Manager 11.1.2

Configure the data source for Access Manager 11.1.2 by completing the following steps:

1. Log in to the Oracle Access Manager 11.1.2 console using the following URL:

   ```
   http://host:port/oamconsole
   ```

   In this URL,

   - *host* refers to the fully qualified domain name of the machine hosting the Oracle Access Manager console (Administration Server)
   - *port* refers to the designated bind port for the Oracle Access Manager console, which is the same as the bind port for the Administration Server

2. Go to the **System Configuration** tab.
3. Select **Common Configuration**.
4. Expand **Data Sources**., and select **User Identity Stores**
5. Under **User Identity Stores**, create a new data source by clicking the **Create** icon on the top of the left panel. This data source must be of type Open LDAP (or OUD). You must specify the user store details of OpenDS of OpenSSO Enterprise 8.0 for this new data source.

## 18.7 Updating LDAPNoPasswordAuthModule in Access Manager 11.1.2

**LDAPNoPasswordAuthModule** is the authentication module used by **OAM10gScheme** that protects `Resource-1`.

You must update the authentication module **LDAPNoPasswordAuthModule** to point to the data source created in Section 18.6 as its **User Identity Store**. To do this, complete the following steps:

1. Log in to the Oracle Access Management 11.1.2 console using the following URL:

   ```
   http://host:port/oamconsole
   ```

In this URL,

- *host* refers to the fully qualified domain name of the machine hosting the Oracle Access Manager console (Administration Server)
- *port* refers to the designated bind port for the Oracle Access Management 11.1.2 console, which is the same as the bind port for the Administration Server

2. Go to the **System Configuration** tab.
3. Expand **Access Manager**, and then expand **Authentication Modules**.
4. Expand **LDAP Authentication Module**.
5. Click **LDAPNoPasswordAuthModule**, and update the User Identity Stores to point to the data source that you created in Section 18.6.

## 18.8 Creating the Profile of Agent-1 in Access Manager 11.1.2

You must create the profile of `Agent-1` in Access Manager 11.1.2, and install a new Policy Agent 3.0 (`Agent-1`) pointing to Access Manager 11.1.2 server.

For information about creating the profile of agent in Access Manager 11.1.2, see "Registering and Managing OpenSSO Policy Agents Using the Console" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.

For information about installing Policy Agent 3.0, see the respective guide in the Sun OpenSSO Enterprise 8.0 Documentation Library.

## 18.9 Creating an Authentication Policy in Access Manager 11.1.2 to Protect Resource-1

Create an authentication policy (referred to as `Policy-2`) under the appropriate Application Domain to protect `Resource-1` with the authentication scheme named **OAM10gAuthScheme**.

Also, create an authorization policy for `Resource-1` with the condition `TRUE`. The resource URLs configured should be `"/"` and `"/.../*"`.

For more information about creating and managing authentication and authorization policies, see "Managing Policies to Protect Resources and Enable SSO" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.

## 18.10 Modifying the OpenSSO Cookie Name in Access Manager 11.1.2

You must change the default cookie name of OpenSSO Cookie in Access Manager 11.1.2 server to a new name in order to avoid conflict between the cookie names of Access Manager 11.1.2 and OpenSSO Enterprise 8.0 servers. To do this, complete the following steps:

1. Open the `*IAM_HOME*/user_projects/domains/base_domain/config/fmwconfig/oam-config.xml`.
2. Under the section **openssoproxy**, modify the value of **openssoCookieName** from the default cookie name **iPlanetDirectoryPro** to a different value (for example, `OAMOpenSSOCookie`).
3. Log in to the Oracle Access Management 11.1.2 console using the following URL:

   ```
   http://host:port/oamconsole
   ```

4. Go to the **System Configuration** tab.
5. Expand **Access Manager**, and then expand **SSO Agents**.
6. Expand **OpenSSO Agents**.
7. Select the required `Agent-1`, and update the cookie name with the new value (for example: **OAMOpenSSOCookie**).
8. Restart the Access Manager 11.1.2 Server.

## 18.11 Updating the Profile of Agent-2 in OpenSSO Enterprise 8.0 Server

After you create a policy on the OpenSSO Enterprise 8.0 Server for Access Manager 11.1.2, you must update the profile of `Agent-2` (that you created in Task 6) in OpenSSO Enterprise 8.0 Server. To do this, complete the following steps:

1. Log in to the OpenSSO Enterprise 8.0 server administration console using the URL:

   ```
   http://host:port/opensso
   ```

   In this URL,

   - `<host>` refers to the fully qualified domain name of the machine hosting the OpenSSO Enterprise 8.0 console (administration server)
   - `<port>` refers to the designated bind port for the OpenSSO Enterprise 8.0 console, which is the same as the bind port for the administration server
2. Go to the **Access Control** tab.
3. Click **/(Top Level Realm)** under **Realm Name** column in **Realms** table.
4. Click the **Agents** tab.
5. Click the **Web/J2EE** tab according to the type of `Agent-2`.
6. Click the `Agent-2`.
7. Click the **Application** tab.
8. Click **Session Attributes Processing**.
9. Select **HTTP_HEADER** as the **Session Attribute Fetch Mode**.
10. Set the value of **OAM_REMOTE_USER** header to **UserToken** to map the session attributes of this agent. To do this, enter **UserToken** as the **Map Key**, and **OAM_REMOTE_USER** as the **Corresponding Map Value** under the **Session Attribute Map**.

## 18.12 Configuring Logout Settings

You must configure logout settings to have single logout across OpenSSO Enterprise 8.0 and Access Manager 11.1.2 in coexistence mode. To do this, you must follow the procedure described in the following two sections:

- Settings to Initiate Logout from OpenSSO Enterprise 8.0 Server
- Settings to Initiate Logout from Access Manager 11.1.2 Server

### 18.12.1 Settings to Initiate Logout from OpenSSO Enterprise 8.0 Server

To initiate logout from the OpenSSO Enterprise 8.0 Server, you must write a post authentication plug-in, and implement `onLogout()` method, and set the query parameter `goto` to the redirect URL `<OAM_server_protocol>://<OAM_server_host>:<OAM_managed_server_port>/opensso/UI/Logout`. This URL redirects the user to the end point URL of the Access Manager 11.1.2 Server.

### 18.12.2 Settings to Initiate Logout from Access Manager 11.1.2 Server

To initiate logout from the Access Manager 11.1.2 Server, you must update the **Logout URL** in the respective Policy Agent 3.0 (`Agent-1`) configured with Access Manager 11.1.2 server to redirect to the OpenSSO Enterprise 8.0 server logout end point. To do this, complete the following steps:

1. Log in to the Oracle Access Management 11.1.2 console using the following URL:

   ```
   http://host:port/oamconsole
   ```

2. Go to the **System Configuration** tab.
3. Expand **Access Manager**, and then expand **SSO Agents**.
4. Expand **OpenSSO Agents**.
5. Select the `Agent-1`, (that is configured with Access Manager 11.1.2 and is protecting `Resource-1`), and set the **Logout URL** to redirect to OpenSSO Enterprise 8.0 server logout end point (`OpenSSO8.x_server_protocol://OpenSSO8.x_server_host:OpenSSO8.x_managed_server_port/opensso/UI/Logout`), with `goto` query parameter set to redirect URL configured for the `Agent-1`.

## 18.13 Verifying the Configuration

To verify the configuration, complete the following steps:

1. Access `Resource-1`. Observe that you are redirected to the OpenSSO Enterprise 8.0 Server for authentication. After the authentication, you can access `Resource-1`.
2. Access any resource protected by `Agent-3` (as shown in Figure 18–1), and observe that an explicit login is required to successfully access the resource.
3. Initiate logout from both OpenSSO Enterprise 8.0 Server and Access Manager 11.1.2 Server, and observe that all the three cookies (**cookie1**, **cookie2**, and **OAM_ID** cookie) are cleared.

# 19

# Coexistence of Sun Java System Access Manager 7.1 with Oracle Access Management Access Manager 11.1.2

This chapter describes how to set up an environment where both Sun Java System Access Manager 7.1 and Oracle Access Management Access Manager (Access Manager) 11*g* Release 2 (11.1.2) deployments coexist, after you migrate from Sun Java System Access Manager 7.1 to Access Manager 11.1.2.

This chapter contains the following sections:

- Coexistence Overview
- Coexistence Topology
- Task Roadmap
- Completing the Prerequisites
- Protecting Access Manager 11g Server's End Point URL by Agent-2
- Configuring Data Source for Access Manager 11.1.2
- Updating LDAPNoPasswordAuthModule in Access Manager 11g
- Migrating the Profile of Agent-1 from Sun Java System Access Manager 7.1 to Access Manager 11.1.2
- Creating an Authentication Policy in Access Manager 11.1.2 to Protect Resource-1
- Changing the Default Cookie Name of Access Manager 11.1.2 Server to a New Name
- Updating the Profile of Agent-2 in Sun Java System Access Manager 7.1 Server
- Configuring Logout Settings
- Verifying the Configuration

## 19.1 Coexistence Overview

During the process of migration from Sun Java System Access Manager 7.1 to Oracle Access Manager 11.1.2, you can have both Sun Java System Access Manager 7.1 and Access Manager 11g deployments coexisting, such that some applications are protected by Sun Java System Access Manager 7.1 while others are protected by Access Manager 11.1.2. It is desirable for end-users to have a seamless single sign-on experience when they navigate between these applications. This is called coexistence mode.

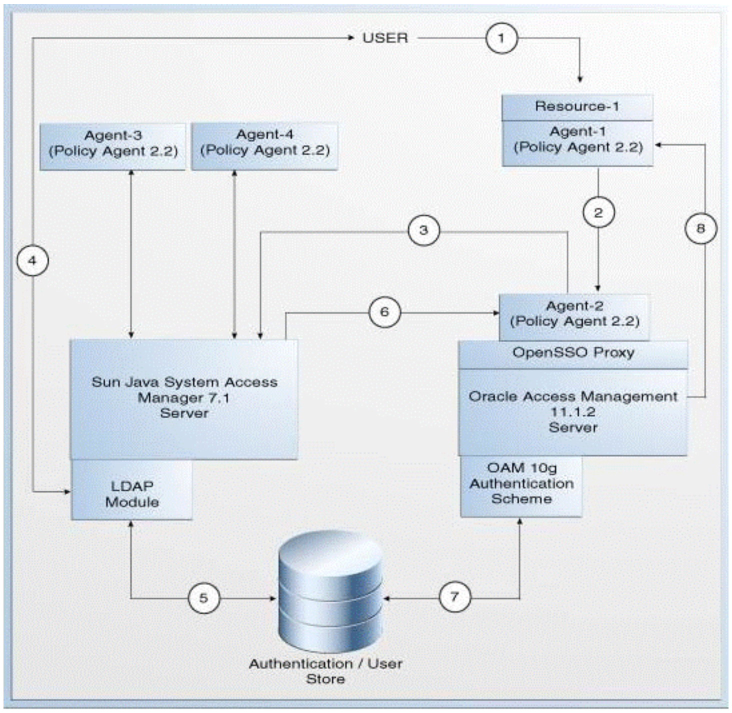
In this mode, Access Manager 11.1.2 protects the migrated applications and any new applications registered with Access Manager 11.1.2; whereas Sun Java System Access Manager 7.1 continues to protect the applications that are not migrated to Access Manager 11.1.2.

In this coexistence mode, Sun Java System Access Manager 7.1 performs the authentication for all the resources protected by Access Manager 11.1.2.

## 19.2 Coexistence Topology

Figure 19–1 illustrates how the authentication is done by the Sun Java System Access Manager 7.1 Server when a user requests to access a protected resource.

***Figure 19–1 Coexistence of Sun Java System Access Manager 7.1 with Access Manager 11.1.2***



The topology consists of disjoint Sun Java System Access Manager 7.1 and Access Manager 11.1.2 environments. The numbers 1-8 in the topology show the sequence in which a request flows in the coexistence environment. See Table 19–1 for the request flow.

### Topology Description

- `Agent-1`: This is the Policy Agent 2.2 that protects `Resource-1`. This agent needs to communicate with Access Manager 11.1.2 Server. You cannot directly register 2.2 agents in Access Manager 11.1.2 Server. Therefore, you must either register `Agent-1` with Sun Java System Access Manager 7.1 and then migrate the profile of this agent from Sun Java System Access Manager 7.1 Server to Access Manager 11.1.2 Server, or you can install a new Policy Agent 3.0 pointing to Access Manager 11.1.2 to protect `Resource-1`.
- `Agent-2`: This is the Policy Agent 2.2 registered with Sun Java System Access Manager 7.1 to protect the end point URL of the Access Manager 11.1.2 Server.

You must create a profile for this agent in Sun Java System Access Manager 7.1 Server and install a new policy agent (2.2).

- `Agent-3` and `Agent-4`: These are the policy agents (2.2) registered with Sun Java System Access Manager 7.1.
- `Resource-1`: This is a resource which is protected by `Agent-1` which talks to the Access Manager 11.1.2 Server.
- `Policy-1`: This is the policy created on Access Manager 11.1.2 server for protecting `Resource-1`. This policy is created as part of the task: Creating an Authentication Policy in Access Manager 11.1.2 to Protect Resource-1.
- `Policy-2`: This is the policy created on Sun Java System Access Manager 7.1 Server for opensso proxy endpoints of Access Manager 11.1.2 protected by `Agent-2`. This policy is created as part of the task: Protecting Access Manager 11g Server's End Point URL by Agent-2.

Table 19–1 describes the request flow. The numbers in the **Step** column correspond to the numbers shown in the topology in Figure 19–1.

***Table 19–1 Request Flow***

| Step | Description |
|---|---|
| 1 | User requests to access `Resource-1` which is protected by `Agent-1` that communicates with the Access Manager 11.1.2 Server. |
| 2 | `Agent-1` redirects the user to Access Manager 11*g* Server for authentication (…`./opensso/UI/Login.....?goto=resource1`) using the authentication scheme **OAM10gAuthScheme** as per `Policy-1`. The user authenticated by Sun Java System Access Manager server is set in the **OAM_REMOTE_USER** header by the OpenSSO agent. Hence, `Agent-1` uses the authentication scheme **OAM10*g*AuthScheme** to assert the user from header **OAM_REMOTE_USER**. |
| 3 | The Access Manager 11.1.2 Server end point is protected by `Agent-2` that communicates with the Sun Java System Access Manager 7.1 Server.<br>Therefore, `Agent-2` redirects the user to the Sun Java System Access Manager 7.1 Server for LDAP authentication (`...opensso/UI/Login?goto=<`…`./oam/server/.....?goto=resource1>`) as per `Policy-2`. |
| 4 | The Sun Java System Access Manager 7.1 server's LDAP authentication module prompts the user for LDAP user name and password. User must enter the valid LDAP credentials. |
| 5 | The Sun Java System Access Manager 7.1 Server validates the user credentials, and creates user session as OpenSSO Enterprise 8.0 session and sets the OpenSSO Enterprise 8.0 SSO **cookie1** with this session ID. |
| 6 | Sun Java System Access Manager 7.1 server redirects the user to the Access Manager 11.1.2 Server (…`./opensso/UI/Login/.....?goto=resource1.` |
| 7 | `Agent-2` verifies the user session and policy evaluation by ensuring the presence of Sun Java System Access Manager 7.1 session cookie 1. It now provides access to Access Manager 11.1.2 Server (…`./opensso/UI/Login/.....?goto=resource1`) after setting the header `OAM_REMOTE_USER` to the `userID` in Session Attribute Mapping.<br>The Access Manager 11.1.2 Server invokes OAM 10g Authentication scheme (**OAM10gAUthScheme**) as per step 2 (`Policy-1`).The Access Manager 11.1.2 server asserts the user using the header `OAM_REMOTE_USER`, using the **OAM10gScheme** configured for the `Resource-1`. |

*Table 19–1 (Cont.) Request Flow*

| Step | Description |
|---|---|
| 8 | The Access Manager 11.1.2 Server creates Access Manager session and sets headers. It also sets the **OAM_ID** cookie and Sun Java System Access Manager SSO **cookie2** (via OpenSSO Proxy), and redirects the user to `Resource-1`. Sun Java System Access Manager 7.1 SSO **cookie2** has link to the related **OAM_ID** cookie.<br>The user can now access `Resource-1`, as `Agent-1` verifies the user session and policy evaluation by ensuring the presence of Sun Java System Access Manager session **cookie2** and **OAM_ID** cookie. |

## 19.3 Task Roadmap

Table 19–2 lists the steps to configure the coexistence environment.

*Table 19–2 Tasks to be Completed*

| Task No | Task | For More Information |
|---|---|---|
| 1 | Understand and get familiar with the coexistence topology before you start the configuration process. | See, Coexistence Topology |
| 2 | Complete the prerequisites. | See, Completing the Prerequisites |
| 3 | Create `Agent-2` profile on the Sun Java System Access Manager 7.1 Server, and install `Agent-2`. Update the web applications `ngsso-web.war` and `openssoproxy-urlmapper.war` in `oam-server.ear` file.<br>Also, create a policy on Sun Java System Access Manager 7.1 to protect the end point URL of Access Manager 11.1.2 Server 11.1.2 by `Agent-2`. | See, Protecting Access Manager 11g Server's End Point URL by Agent-2 |
| 4 | Configure the data sources for Access Manager 11.1.2. | See, Configuring Data Source for Access Manager 11.1.2 |
| 5 | Update the authentication module in Access Manager 11*g*, and point the user identity store to the data source that is configured in Section 19.6. | See, Updating LDAPNoPasswordAuthModule in Access Manager 11g |
| 6 | Migrate the profile of `Agent-1` from Sun Java System Access Manager 7.1 to Access Manager 11.1.2. | See, Migrating the Profile of Agent-1 from Sun Java System Access Manager 7.1 to Access Manager 11.1.2 |

*Table 19–2 (Cont.) Tasks to be Completed*

| Task No | Task | For More Information |
|---|---|---|
| 7 | Create an authentication policy on the Access Manager 11.1.2 Server to protect `Resource-1`. | See, Creating an Authentication Policy in Access Manager 11.1.2 to Protect Resource-1 |
| 8 | Change the default cookie name of Access Manager 11.1.2, so that the cookie names of Access Manager 11*g* and Sun Java System Access Manager 7.1 are different. | See, Changing the Default Cookie Name of Access Manager 11.1.2 Server to a New Name |
| 9 | Update the profile of `Agent-2` in Sun Java System Access Manager 7.1 Server with the right Session Attributes Mapping. | See, Updating the Profile of Agent-2 in Sun Java System Access Manager 7.1 Server |
| 10 | Configure logout setting to initiate logout from both Sun Java System Access Manager 7.1 Server and Access Manager 11.1.2 Server. | See, Configuring Logout Settings |
| 11 | Verify the configuration. | See, Verifying the Configuration |

## 19.4 Completing the Prerequisites

Complete the following prerequisites before you start performing the tasks described in this chapter:

- Read the Oracle Fusion Middleware System Requirements and Specifications document to ensure that your environment meets the minimum requirements for the products you are installing, upgrading, and migrating.

  **Note:** For information about Oracle Fusion Middleware concepts and directory structure, see "Understanding Oracle Fusion Middleware Concepts and Directory Structure" in the *Oracle Fusion Middleware Installation Planning Guide for Oracle Identity and Access Management*.

- Verify that the version of Sun Java System Access Manager that you are using is supported for coexistence. For more information about supported starting points for OpenSSO coexistence, see Section 11.9, "Supported Starting Points for Coexistence of Sun Java System Access Manager With Oracle Access Management Access Manager 11.1.2".

- Ensure that the Sun Java System Access Manager 7.1 and Oracle Access Management Access Manager 11*g* Release 2 (11.1.2) installations are complete, and the servers are running.

  If you have not installed and configured Oracle Access Management Access Manager 11*g* Release 2 (11.1.2), you must do it before you start with the next task.

For more information on installing and configuring Oracle Access Management Access Manager 11*g* Release 2 (11.1.2), see "Installing Oracle Identity and Access Management (11.1.2.0.0)" and "Configuring Oracle Access Management" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

- Ensure that the Sun Java System Access Manager 7.1 and Access Manager 11.1.2 share the same user store.
- If Sun Java System Access Manager 7.1 and Access Manager 11.1.2 servers are running on different machines, make sure that the time of these machines are synchronized.

## 19.5 Protecting Access Manager 11*g* Server's End Point URL by Agent-2

You must create a profile for `Agent-2` in Sun Java System Access Manager 7.1, and freshly install a policy agent 2.2 to protect the end point URL of the Access Manager 11.1.2 Server. Also, you must create a policy for protecting the end-point URL of the Access Manager 11*g* Server in the Sun Java System Access Manager 7.1 Server. To do this, perform the following tasks:

1. Creating the Profile of Agent-2 for Access Manager on Sun Java System Access Manager 7.1 Server
2. Installing Agent-2 (Policy Agent 2.2)
3. Updating Web Applications to Include Agent Filter Configurations
4. Creating Policy on Sun Java System Access Manager 7.1 Server for Access Manager

### 19.5.1 Creating the Profile of Agent-2 for Access Manager on Sun Java System Access Manager 7.1 Server

Create `Agent-2` profile (as shown in Figure 19–1) on the Sun Java System Access Manager 7.1 Server by doing the following:

1. Log in to the Sun Java System Access Manager 7.1 server console using the URL:

   ```
   http://host:port/amserver
   ```

   In this URL,

   - *`host`* refers to fully qualified domain name of the machine hosting the Sun Java System Access Manager 7.1 console (administration server)
   - *`port`* refers to the designated bind port for the Sun Java System Access Manager 7.1 console
2. Go to the **Access Control** tab.
3. Click the top realm under **Realm Name** column in **Realms** table.
4. Go to the **Subjects** tab, and click the **Agent** tab.
5. Click **New** to create the new `Agent-2`, and specify the necessary details about the agent.
6. Click **OK**.

### 19.5.2 Installing Agent-2 (Policy Agent 2.2)

Install `Agent-2` (Policy Agent 2.2) in front of Access Manager.

For more information about installing Policy Agent 2.2, see "Installing the Policy Agent for WebLogic Server/Portal 10" in the *Sun Java System Access Manager Policy Agent 2.2 Guide for BEA WebLogic Server/Portal 10*.

### 19.5.3 Updating Web Applications to Include Agent Filter Configurations

Update the web applications `ngsso-web.war` and `openssoproxy-urlapper.war` to include the agent filter configurations in the `web.xml` file for the Access Manager 11.1.2 Server to be protected by `Agent-2`. To do this, complete the following steps:

1. Unzip the `oam-server.ear` file from the location *`IAM_HOME`*`/oam/server/apps/oam-server.ear`, and extract the contents to a temporary directory.
2. Extract the contents of the `ngsso-web.war` file, and then extract the contents of `web.xml` file. Update the `web.xml` file with the appropriate agent filter configuration for the Access Manager 11.1.2 server to be protected by `Agent-2`. Update the filter definition with the URL `/server/opensso/login/*` in `url-pattern`.

   For example:

   ```
   <filter>
   <filter-name>Agent</filter-name>
   <filter-class>com.sun.identity.agents.filter.AmAgentFilter</filter-class>
   </filter>
   <filter-mapping>
   <filter-name>Agent</filter-name>
   <url-pattern>/server/opensso/login/*</url-pattern>
   </filter-mapping>
   ```

3. Extract the contents of the `openssoproxy-urlmapper.war` file at the same location *`IAM_HOME`*`/oam/server/apps/oam-server.ear`. Update the `web.xml` file with the appropriate agent filter configuration for the Access Manager 11.1.2 Server to be protected by `Agent-2`. Update the filter definition with the URL `/UI/*` in `url-pattern`.

   For example:

   ```
   <filter>
   <filter-name>Agent</filter-name>
   <filter-class>com.sun.identity.agents.filter.AmAgentFilter</filter-class>
   </filter>
   <filter-mapping>
   <filter-name>Agent</filter-name>
   <url-pattern>/UI/*</url-pattern>
   </filter-mapping>
   ```

4. Re-package the `oam-server.ear` file to include the updated `ngsso-web.war` and `openssoproxy-urlapper.war` files.
5. Redeploy the updated `oam-server.ear` file.

### 19.5.4 Creating Policy on Sun Java System Access Manager 7.1 Server for Access Manager

You must create an policy (referred to as `Policy-1`) on Sun Java System Access Manager 7.1 Server to protect the end point URL of the Access Manager 11.1.2 server. To do this, complete the following steps:

1. Log in to the Sun Java System Access Manager 7.1 Server console using the URL:

   `http://`*`host`*`:`*`port`*`/amserver`

   In this URL,

   - *`host`* refers to the fully qualified domain name of the machine hosting the Sun Java System Access Manager 7.1 console (administration server).
   - *`port`* refers to the designated bind port for the Sun Java System Access Manager 7.1 console, which is the same as the bind port for the administration server.

2. Click the **Access Control** tab.
3. Click the top realm under **Realm Name** column in **Realms** table.
4. Click the **Policies** tab.
5. Click **New Policy**, and provide the details of the new policy for protecting the end point URL of Access Manager 11.1.2 Server with **Rule** as *`OAM_server_protocol`*`://`*`OAM_server_host`*`:`*`OAM_managed_server_port`*`/opensso/UI/Login*?*`, and *`OAM_server_protocol`*`://`*`OAM_managed_server_host`*`:`*`OAM_managed_server_port`*`/oam/server/opensso/login*`, and **Subject** as **Authenticated Users**.
6. Click **OK**.

## 19.6 Configuring Data Source for Access Manager 11.1.2

Configure the data source for Access Manager 11.1.2 by completing the following steps:

1. Log in to the Oracle Access Manager 11.1.2 console using the following URL:

   `http://`*`host`*`:`*`port`*`/oamconsole`

   In this URL,

   - *`host`* refers to the fully qualified domain name of the machine hosting the Oracle Access Manager console (administration server).
   - *`port`* refers to the designated bind port for the Oracle Access Management 11.1.2 console, which is the same as the bind port for the administration server

2. Go to the **System Configuration** tab.
3. Select **Common Configuration**.
4. Expand **Data Sources**, and select **User Identity Stores**
5. Under **User Identity Stores**, create a new data source by clicking the **Create** icon on the top of the left panel. This data source must be of type `ODSEE`. You must provide the details of the Sun Java System Directory Server used by Sun Java System Access Manager 7.1 as configuration and user store.

## 19.7 Updating LDAPNoPasswordAuthModule in Access Manager 11*g*

You must update the authentication module used by **OAM10gScheme** to point to the data source created in section 20.6 as its **User Identity Store**. To do this, complete the following steps:

1. Log in to the Oracle Access Management 11.1.2 console using the following URL:

   ```
   http://host:port/oamconsole
   ```

2. Go to the **System Configuration** tab.
3. Expand **Access Manager**, and then expand **Authentication Modules**.
4. Expand **LDAP Authentication Module**.
5. Click **LDAPNoPasswordAuthModule**, and update the user identity stores to point to the data source that you created in Section 19.6.

## 19.8 Migrating the Profile of Agent-1 from Sun Java System Access Manager 7.1 to Access Manager 11.1.2

`Agent-1` is the Policy Agent (2.2) that protects `Resource-1`. This agent should be a 2.2 Web Agent, and should communicate with the Access Manager 11.1.2 Server. But the 2.2 agents cannot be directly created in Access Manager 11.1.2. Therefore, you must register `Agent-1` with Sun Java System Access Manager 7.1, and then migrate the profile of `Agent-1` from the Sun Java System Access Manager 7.1 Server to Access Manager 11.1.2 Server.

For information on migrating the profile of `Agent-1` from Sun Java System Access Manager 7.1 to Access Manager 11.1.2, see Chapter 16, "Migrating Sun Java System Access Manager 7.1 Environments".

> **Note:** When completing the procedure to migrate the profile of `Agent-1` to Access Manager 11.1.2, update the agent profile of `Agent-1` alone in section 17.7.3 "Updating the Agent Profile for 2.2 Agents", since you need to migrate `Agent-1` alone.
>
> Make sure you do not create any policies protecting the resources that are intercepted by `Agent-1` (or resources on this agent's host or port) in Sun Java System Access Manager 7.1.
>
> If you do not wish to migrate the profile of `Agent-1` (Web Agent 2.2) to Access Manager 11.1.2, you can create the profile of `Agent-1` in Access Manager 11.1.2, and install a new Policy Agent 3.0 pointing to the Access Manager 11.1.2 Server to protect `Resource-1`.

If `Agent-1` is a 2.2 J2EE Agent, you must create the profile of `Agent-1` in Access Manager 11.1.2, and install a new Policy 3.0 J2EE Agent pointing to the Access Manager 11.1.2 Server to protect `Resource-1`. This is because, the migration of 2.2 J2EE Agents to Access Manager 11.1.2, and the creation of 2.2 agents in Access Manager 11.1.2 are not supported.

For information about creating the profile of agent in Access Manager 11.1.2, see "Registering and Managing OpenSSO Policy Agents Using the Console" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.

For information about installing Policy Agent 3.0, see the respective guide in the Sun OpenSSO Enterprise 8.0 Documentation Library.

## 19.9 Creating an Authentication Policy in Access Manager 11.1.2 to Protect Resource-1

Create an authentication policy (referred to as `Policy-2`) under the appropriate application domain to protect `Resource-1` with the authentication scheme named **OAM10gScheme**.

Also, create an authorization policy for `Resource-1` with the condition `TRUE`. The resource URLs configured should be `"/"` and `"/.../*"`.

For more information on creating and managing authentication and authorization policies, see "Managing Policies to Protect Resources and Enable SSO" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.

## 19.10 Changing the Default Cookie Name of Access Manager 11.1.2 Server to a New Name

You must change the default cookie name of the Access Manager 11.1.2 Server to a new name in order to avoid conflict between the cookie names of Access Manager 11.1.2 and Sun Java System Access Manager 7.1 servers. To do this, complete the following steps:

1. Stop the WebLogic Administration Server and the Access Manager 11.1.2 Managed Servers.

   For more information about stopping the Administration Server and the Managed Servers, see "Starting and Stopping Administration Servers" and "Starting and Stopping Managed Servers" in the *Oracle Fusion Middleware Administrator's Guide*.

2. Open the `oam-config.xml` file from the location *`IAM_HOME`*`/user_projects/domains/base_domain/config/fmwconfig/oam-config.xml`.

3. Increment the value of the parameter **Version** by one in the `oam-config.xml` file.

4. Under the section **openssoproxy**, modify the value of **openssoCookieName** from the default cookie name **iPlanetDirectoryPro** to a different value (for example: **OAMSAMCookie**).

5. Start the WebLogic Administration Server and the Access Manager 11.1.2 Managed Servers.

   For more information about starting the Administration Server and the Managed Servers, see "Starting and Stopping Administration Servers" and "Starting and Stopping Managed Servers" in the *Oracle Fusion Middleware Administrator's Guide*.

6. Log in to the Oracle Access Management 11.1.2 console using the following URL:

   ```
   http://host:port/oamconsole
   ```

7. Go to the **System Configuration** tab.

8. Expand **Access Manager**, and then expand **SSO Agents**.

9. Expand **OpenSSO Agents**.

10. Select the required `Agent-1`, and update the cookie name with the new value (for example, **OAMSAMCookie**).

11. Restart the Access Manager 11.1.2 Server.

## 19.11 Updating the Profile of Agent-2 in Sun Java System Access Manager 7.1 Server

You must update the Session Attribute Mapping for `Agent-2` to set the header `OAM_REMOTE_USER` to the value of `UserToke` in `AMAgent.properties` file. To do this, complete the following steps:

1. Open the `AMAgent.properties` file from the location where you installed `Agent-2`.
2. Set the following values in the properties file:
   - `com.sun.identity.agents.config.session.attribute.fetch.mode=HTTP_HEADER`
   - `com.sun.identity.agents.config.session.attribute.mapping[UserToken]=OAM_REMOTE_USER`
3. Restart the web container instance of `Agent-2`.

## 19.12 Configuring Logout Settings

You must configure logout settings to have single logout across Sun Java System Access Manager 7.1 and Access Manager 11.1.2 in coexistence mode. To do this, you must follow the procedure described in the following two sections:

- Settings to Initiate Logout from Sun Java System Access Manager 7.1 Server
- Settings to Initiate Logout from Access Manager 11g Server

### 19.12.1 Settings to Initiate Logout from Sun Java System Access Manager 7.1 Server

To initiate logout from Sun Java System Access Manager 7.1 Server, you must write a post authentication plug-in, and implement `onLogout()` method, and set the query parameter `goto` to the redirect URL `<OAM_server_protocol>://<OAM_server_host>:<OAM_managed_server_port>/opensso/UI/Logout`. This redirects the user to the end point URL of the Access Manager 11.1.2 server.

### 19.12.2 Settings to Initiate Logout from Access Manager 11*g* Server

To initiate logout from the Access Manager 11.1.2 server, you must update the **Logout URL** in the respective Policy Agent 2.2 (`Agent-1`) configured with Access Manager 11.1.2 Server to redirect to the Sun Java System Access Manager 7.1 Server logout end point. To do this, complete the following steps:

1. Log in to the Oracle Access Management 11.1.2 console using the following URL:

   ```
   http://host:port/oamconsole
   ```

2. Go to the **System Configuration** tab.
3. Expand **Access Manager**, and then expand **SSO Agents**.
4. Expand **OpenSSO Agents**.
5. Select the `Agent-1`, (that is configured with Access Manager 11*g* and is protecting `Resource-1`), and set the **Logout URL** to redirect to Sun Java System Access Manager 7.1 server logout end point (`*SAM7.1_server_protocol*://*SAM7.1_server_host*:*SAM7.1_managed_server_port*/amserver/UI/Logout`), with `goto` query parameter set to the redirect URL configured for `Agent-1`.

For example: If the Logout URL already configured is *protocol*://*OAMHOST*:*OAMPORT*/opensso/UI/Logout, it must be modified to *protocol*://*OAMHOST*:*OAMPORT*/*opensso*/UI/Logout?goto=*SAM7.1_server_protocol*://*SAM7.1_server_host*:*SAM7.1_server_port*/amserver/UI/Logout?goto=*any url agent wants to be redirected to after logout*

## 19.13 Verifying the Configuration

To verify the configuration, complete the following steps:

1. Access Resource-1. Observe that you are redirected to the Sun Java System Access Manager 7.1 server for authentication. After the authentication, you can access Resource-1.
2. Access any resource protected by Agent-3 (as shown in Figure 19–1), and observe that an explicit login is required to access the resource.
3. Initiate logout from both the Sun Java System Access Manager 7.1 Server and Access Manager 11.1.2 Server, and observe that all the three cookies (**cookie1**, **cookie2**, and **OAM_ID** cookie) are cleared.