Oracle® Fusion Middleware

Upgrade Guide for Oracle Identity and Access Management

11*g* Release 1 (11.1.1.7.0)

E27996-01

March 2013

Oracle Fusion Middleware Upgrade Guide for Oracle Identity and Access Management, 11*g* Release 1 (11.1.1.7.0)

E27996-01

Primary Author: Shynitha K S

Contributors: Allison Sparshott, Deepak Ramakrishnan, Gururaj B S, Madhu Martin, Mark Karlstrand, Nagasravani Akula, Niranjan Ananthapadmanabha, Peter Laquerre, Ramya Subramanya, Ravi Thirumalasetty, Sitaraman Swaminathan, Sree Chitturi, Srinivas Nagandla, Stuart Duggan, Venu Shastri

Contents

4 Upgrading Oracle Adaptive Access Manager 10*g* Environments

Preface

This document describes how to upgrade Oracle Single Sign-On 10*g* and Oracle Identity Management 10g to Oracle Identity and Access Management 11*g* Release 1 (11.1.1.7.0).

Audience

This document is intended for administrators who are responsible for upgrading Oracle Single Sign-On 10*g* and Oracle Identity Management components to Oracle Identity and Access Management 11*g* Release 1 (11.1.1.7.0).

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 1 (11.1.1.7.0) 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*
- *Oracle Fusion Middleware Upgrade Guide for Oracle Identity Management*

Conventions

The following text conventions are used in this document:

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

Part I

Understanding Oracle Identity and Access Management

This part includes the following chapters:

1 Introduction

This chapter provides an overview of Oracle Identity and Access Management 11*g* Release 1 (11.1.1.7.0). This chapter includes the following topics:

- Oracle Identity and Access Management Overview
- Components That can be Upgraded to Oracle Identity and Access Management 11g Release 1 (11.1.1.7.0)
- Flow Chart of Oracle Single Sign-On and Oracle Identity and Access Management Upgrade Processes
- Task Roadmap

1.1 Oracle Identity and Access Management Overview

Oracle Identity and Access Management enables enterprises to manage the end-to-end lifecycle of user identities across all enterprise resources—both within and beyond the firewall. With Oracle Identity Management and 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 Corporation leads the industry with award-winning Identity Management offerings that constitute the most comprehensive solution offered by any vendor, including:

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

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

`http://www.oracle.com/identity`

Oracle Identity and Access Management 11*g* Release 1 (11.1.1.7.0) installer includes the following components:

- Oracle Access Manager
- Oracle Adaptive Access Manager
- Oracle Identity Manager
- Oracle Entitlements Server
- Oracle Identity Navigator

1.2 Components That can be Upgraded to Oracle Identity and Access Management 11*g* Release 1 (11.1.1.7.0)

You can upgrade the following 10*g* components to Oracle Identity and Access Management 11*g* Release 1 (11.1.1.7.0):

- Oracle Adaptive Access Manager
- Oracle Single Sign-On

> **Note:** Oracle Single Sign-On and Oracle Delegated Administration Services Release 10*g* are required components for Oracle Portal, Forms, Reports, and Discoverer in 10*g* Release and 11*g* Release.
>
> There are no 11*g* Release 1 (11.1.1.7.0) versions of Oracle Single Sign-On and Oracle Delegated Administration Services.
>
> If you are running Oracle Single Sign-On or Oracle Delegated Administration Services Release 10*g*, you can upgrade to Oracle Access Manager 11*g*, as described in Chapter 3, "Upgrading Oracle Single Sign-On 10g Environments".

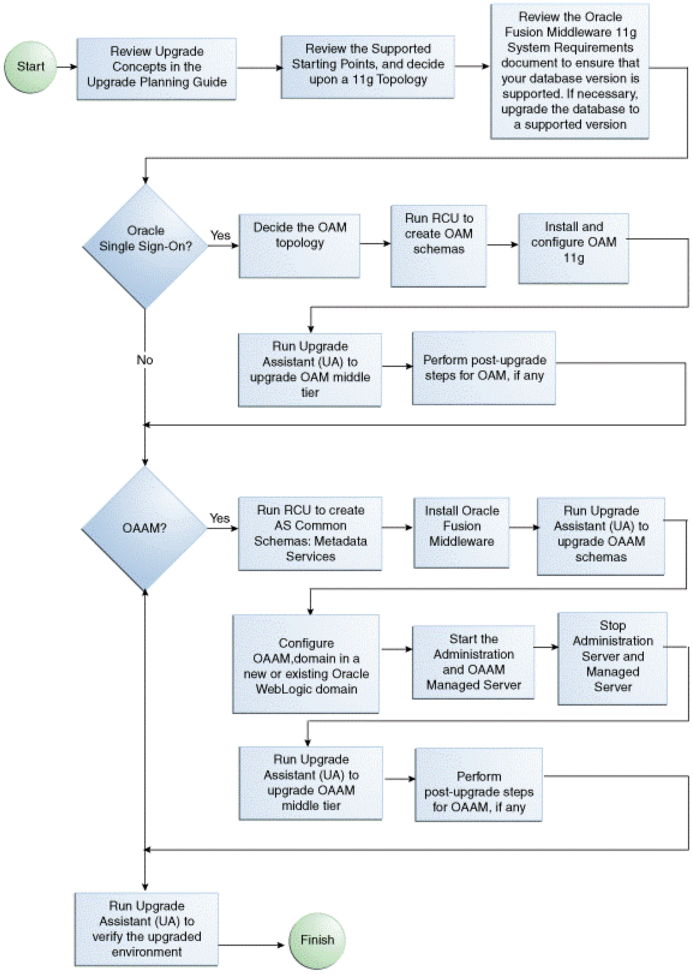
For upgrading to Oracle Identity and Access Management 11*g*, you must follow the procedures described in Part II, "Upgrading Oracle Single Sign-On and Oracle Adaptive Access Manager to 11.1.1.7.0".

> **Note:** If you wish to upgrade the Oracle Identity Management components like Oracle Internet Directory (OID), Oracle Virtual Directory (OVD), or Oracle Identity Federation (OIF), refer to the *Oracle Fusion Middleware Upgrade Guide for Oracle Identity Management*.

1.3 Flow Chart of Oracle Single Sign-On and Oracle Identity and Access Management Upgrade Processes

Figure 1–1 provides a flow chart of the Oracle Single Sign-On and Oracle Adaptive Access Manager upgrade process. Review this chart to get familiar with the steps you will be required to take, based on your existing version of Oracle Single Sign-On and Oracle Adaptive Access Manager.

Figure 1–1 Flow Chart of the Oracle Single Sign-On and Oracle Adaptive Access Manager Upgrade Processes


Start
Review Upgrade Concepts in the Upgrade Planning Guide
Review the Supported Starting Points, and decide upon a 11g Topology
Review the Oracle Fusion Middleware 11g System Requirements document to ensure that your database version is supported. If necessary, upgrade the database to a supported version
Oracle Single Sign-On?
Yes
Decide the OAM topology
Run RCU to create OAM schemas
Install and configure OAM 11g
Run Upgrade Assistant (UA) to upgrade OAM middle tier
Perform post-upgrade steps for OAM, if any
No
OAAM?
Yes
Run RCU to create AS Common Schemas: Metadata Services
Install Oracle Fusion Middleware
Run Upgrade Assistant (UA) to upgrade OAAM schemas
Configure OAAM,domain in a new or existing Oracle WebLogic domain
Start the Administration and OAAM Managed Server
Stop Administration Server and Managed Server
Run Upgrade Assistant (UA) to upgrade OAAM middle tier
Perform post-upgrade steps for OAAM, if any
Run Upgrade Assistant (UA) to verify the upgraded environment
Finish

1.4 Task Roadmap

Table 1–1 describes each of the steps in the upgrade process flow chart, which is shown in Figure 1–1. The table also provides information on where to get more information on each step in the process.

Table 1–1 Steps Involved in the Upgrade Process

Step	Description	For More Information, see
Review Upgrade Concepts in the Upgrade Planning Guide.	The *Oracle Fusion Middleware Upgrade Planning Guide* provides a high-level overview of how to upgrade your entire Oracle Application Server environment to Oracle Fusion Middleware. It includes compatibility information and instructions for upgrading any databases that support your middleware components.	*Oracle Fusion Middleware Upgrade Planning Guide*
Review the Supported Starting Points and 11*g* Topologies.	Before starting your upgrade, you should be familiar with the new features, supported started points, and recommended topologies for Oracle Fusion Middleware 11*g*. Based this knowledge, you can then decide upon an 11*g* topology.	Chapter 2, "Upgrade Starting Points"
If necessary, upgrade the Identity Management database to a supported database version.	When you upgrade to Oracle Fusion Middleware 11*g*, the OracleAS Identity Management schemas are upgraded to 11*g*. As a result, before you upgrade, you must be sure the database that hosts the schemas is a supported version.	*Oracle Fusion Middleware Upgrade Planning Guide*
Oracle Single Sign-On?	You can only upgrade Oracle Single Sign-On to Oracle Access Manager, then be sure to follow the appropriate instructions in this guide.	Chapter 3, "Upgrading Oracle Single Sign-On 10g Environments"
Install and Configure Oracle Access Manager 11*g*.	Install and configure an instance of Oracle Access Manager 11*g* on the same host as the Oracle Application Server 10*g* installation or you can use a new host.	Section 3.10, "Installing and Configuring the Oracle Access Manager 11.1.1.7.0 Middle Tier"
Use Upgrade Assistant to Upgrade Oracle Access Manager middle tier.	Run the Upgrade Assistant from your new 11*g* Oracle home and upgrade the Oracle Single Sign-On 10*g*.	Section 3.11, "Upgrading Oracle Access Manager 11.1.1.7.0 Middle Tier Using Upgrade Assistant"

Table 1–1 (Cont.) Steps Involved in the Upgrade Process

Step	Description	For More Information, see
Perform any Post-Upgrade Oracle Access Manager Tasks.	The Upgrade Assistant automates many of the upgrade procedures, but in some cases, there are additional, manual tasks that you might have to perform.	Section 3.12, "Post-Upgrade Tasks"
Oracle Adaptive Access Manager?	If you are upgrading Oracle Adaptive Access Manager, then be sure to follow the appropriate instructions in this guide.	Chapter 4, "Upgrading Oracle Adaptive Access Manager 10g Environments"
Install and Configure Oracle Adaptive Access Manager 11*g*.	Install and configure an instance of Oracle Adaptive Access Manager 11*g* on the same host as the Oracle Application Server 10*g* installation.	Section 4.6, "Task 4: Install Oracle Fusion Middleware"
Use Upgrade Assistant to Upgrade Oracle Adaptive Access Manager schema and middle tier.	Run the Upgrade Assistant from your new 11*g* Oracle home and upgrade the Oracle Adaptive Access Manager schemas and middle tiers.	Section 4.7, "Task 5: Use Upgrade Assistant to Upgrade the Oracle Adaptive Access Manager Schema" Section 4.11, "Task 9: Use Upgrade Assistant to Upgrade Oracle Adaptive Access Manager Middle Tier"
Perform any Post-Upgrade Oracle Adaptive Access Manager Tasks.	The Upgrade Assistant automates many of the upgrade procedures, but in some cases, there are additional, manual tasks that you might have to perform.	Section 4.13, "Task 11: Complete Any Required Oracle Adaptive Access Manager Post-Upgrade Tasks"
Complete the post-upgrade tasks for Oracle Single Sign-On upgrade. Also, verify the Oracle Adaptive Access Manager upgrade.	You can use the Upgrade Assistant to validate the upgrade and verify that the upgraded environment is up and running successfully.	Section 3.12, "Post-Upgrade Tasks" Section 4.14, "Task 12: Verify the Oracle Adaptive Access Manager Upgrade"

2 Upgrade Starting Points

This chapter describes the supported starting points for Oracle Identity and Access Management upgrade. This chapter contains the following sections:

- Supported Upgrade Starting Points for Oracle Access Manager
- Supported Upgrade Starting Points for Oracle Adaptive Access Manager

> **Note:** The starting point patchsets listed in this chapter were the latest patchsets available at the time this guide was published.
>
> For a list of the latest patchsets available for your installation, refer to *My Oracle Support*.

2.1 Supported Upgrade Starting Points for Oracle Access Manager

This guide provides instructions for upgrading from the Oracle Single Sign-On and Oracle Access Manager releases described in Table 2–1.

Table 2–1 Oracle Access Manager Releases Supported By This Guide

Release	Description or Notes
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).

2.2 Supported Upgrade Starting Points for Oracle Adaptive Access Manager

This guide provides instructions for upgrading from the Oracle Adaptive Access Manager releases described in Table 2–2.

Table 2–2 Oracle Adaptive Access Manager Releases Supported By This Guide

Release	Description or Notes	Latest Patchset
10*g* (10.1.4.5)	This version of Oracle Adaptive Access Manager was available as a standalone product.	Bundle Patch 7 Oracle Adaptive Access Manager 10*g* (10.1.4.5.2) is the latest patchset release.

Part II

Upgrading Oracle Single Sign-On and Oracle Adaptive Access Manager to 11.1.1.7.0

This part includes the following chapters:

- Chapter 3, "Upgrading Oracle Single Sign-On 10g Environments"
- Chapter 4, "Upgrading Oracle Adaptive Access Manager 10g Environments"

3 Upgrading Oracle Single Sign-On 10*g* Environments

This chapter describes how to upgrade your existing Oracle Single Sign-On 10*g* to Oracle Access Manager 11*g* Release 1 (11.1.1.7.0).

This chapter contains the following sections:

3.1 Upgrade Overview

The process of upgrading Oracle Single Sign-On 10*g* to Oracle Access Manager 11.1.1.7.0 involves installing Oracle Identity and Access Management 11.1.1.7.0, configuring Oracle Access Manager 11.1.1.7.0, and upgrading the Oracle Access Manager middle tier. Oracle Single Sign-On 10*g* to Oracle Access Manager 11.1.1.7.0 upgrade has three scenarios:

- Oracle Delegated Administration Services required after upgrading Oracle Single Sign-On 10*g* to Oracle Access Manager 11.1.1.7.0
- Oracle Delegated Administration Services required, but Oracle Single Sign-On admin not required after upgrading Oracle Single Sign-On 10*g* to Oracle Access Manager 11.1.1.7.0
- Oracle Delegated Administration Services not required after upgrading Oracle Single Sign-On 10*g* to 11.1.1.7.0

Depending upon the scenario you choose, you must perform the corresponding tasks listed in Upgrade Roadmap.

3.2 Upgrade Summary

You can use Oracle Fusion Middleware Upgrade Assistant to upgrade 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

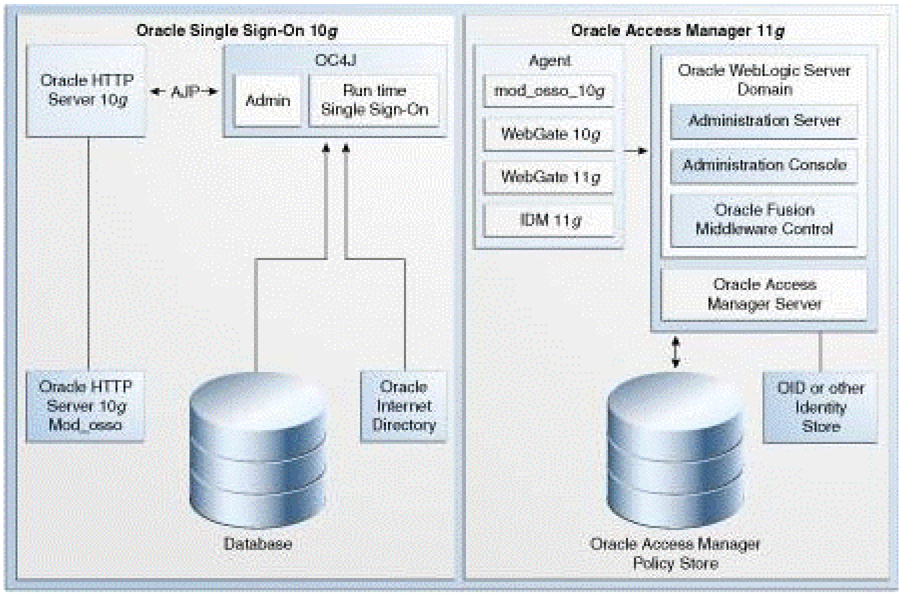
The following components are not upgraded to Oracle Access Manager 11.1.1.7.0 environment when you run Upgrade Assistant to upgrade from Oracle Single Sign-On 10*g*:

- 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.

3.3 Topology Comparison

Figure 3–1 compares a typical Oracle Single Sign-On topology in Oracle Application Server 10*g* with a Oracle Access Manager topology in Oracle Fusion Middleware 11*g*.

Figure 3–1 Comparison of Typical Oracle Single Sign-On Topologies in Oracle Application Server 10g and Oracle Fusion Middleware 11g


Oracle Single Sign-On 10g
Oracle HTTP Server 10g
AJP
OC4J
Admin
Run time Single Sign-On
Oracle HTTP Server 10g Mod_osso
Database
Oracle Internet Directory
Oracle Access Manager 11g
Agent
mod_osso_10g
WebGate 10g
WebGate 11g
IDM 11g
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

3.4 Upgrade Scenarios

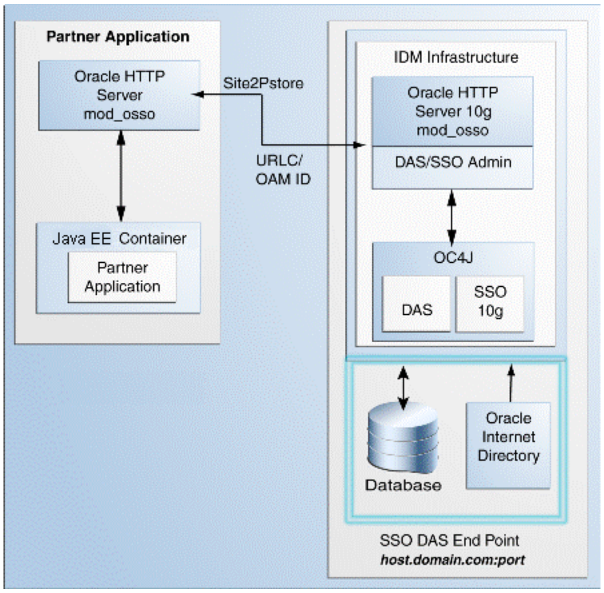
Before you upgrade Oracle Single Sign-On 10*g* to Oracle Access Manager 11.1.1.7.0, you must consider your Oracle Single Sign-On 10*g* infrastructure (Figure 3–2) and depending on the functionality you choose to retain, you must select one of the following scenarios:

- Oracle Delegated Administration Services Required After Upgrading Oracle Single Sign-On 10g to Oracle Access Manager 11.1.1.7.0
- Oracle Delegated Administration Services Required, but Oracle Single Sign-On Admin Not Required After Upgrading Oracle Single Sign-On to Oracle Access Manager 11.1.1.7.0
- Oracle Delegated Administration Services Not Required After Upgrading Oracle Single Sign-On to Oracle Access Manager 11.1.1.7.0

Oracle Single Sign-On 10*g* Infrastructure Before Upgrade

Figure 3–2 illustrates the Oracle Single Sign-On 10*g* topology.

Figure 3–2 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 upgrade scenarios and their Oracle Single Sign-On endpoints.

3.4.1 Oracle Delegated Administration Services Required After Upgrading Oracle Single Sign-On 10*g* to Oracle Access Manager 11.1.1.7.0

Use this upgrade scenario if you want to continue to use the Oracle Delegated Administration Services (DAS) application and the Oracle Single Sign-On Admin tool after upgrading from Oracle Single Sign-On 10*g* to Oracle Access Manager 11.1.1.7.0. Figure 3–3 illustrates the scenario.

Note the following points when using this upgrade scenario:

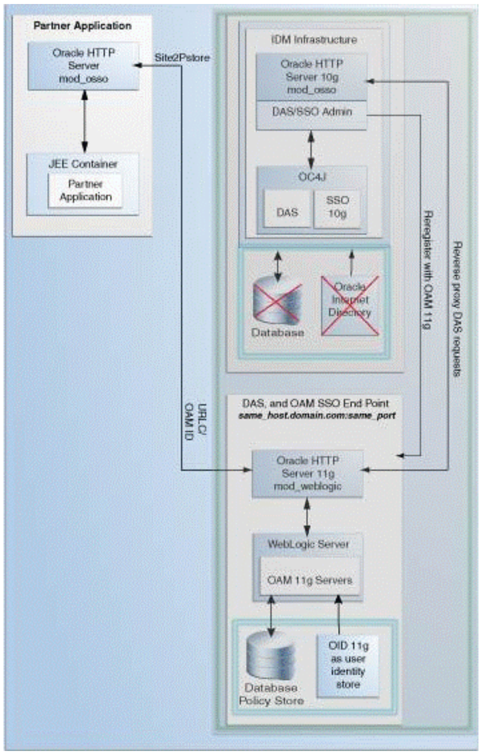
- Use this scenario if you are using Oracle Portal partner applications because you require Oracle Delegated Administration Services and Oracle Single Sign-On Administration. Upgrade all the partner applications at once.
- You are using the same Oracle HTTP Server 10*g* port that front-ended Oracle Single Sign-On 10*g* as the new port for Oracle Access Manager 11.1.1.7.0. Therefore, the Oracle Single Sign-On 10*g* server is no longer accessed. Instead, partner applications use Oracle Access Manager 11.1.1.7.0.

- 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 11.1.1.7.0 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 upgrade, Oracle Internet Directory is selected as the user identity store automatically.

Figure 3–3 Oracle Delegated Administration Services Required After Upgrading 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 upgrade scenario, follow the steps listed in Table 3–1.

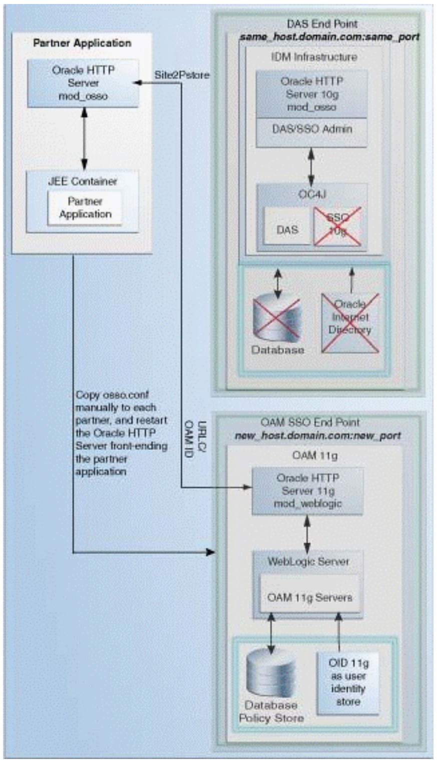
3.4.2 Oracle Delegated Administration Services Required, but Oracle Single Sign-On Admin Not Required After Upgrading Oracle Single Sign-On to Oracle Access Manager 11.1.1.7.0

Use this upgrade scenario if you do not require the Oracle Single Sign-On Admin tool application, but you require the Oracle Delegated Administration Services application after upgrading from Oracle Single Sign-On 10*g* to Oracle Access Manager 11.1.1.7.0. Figure 3–4 illustrates the scenario.

Note the following points when using this upgrade scenario:

- You are using the OHS 10*g* port for Oracle Delegated Administration Services. Therefore, you must install Oracle Access Manager 11.1.1.7.0 on a different machine.
- Upgrade your partner applications in a phased manner.
- Oracle Single Sign-On will no longer work after the upgrade. However, Oracle Delegated Administration Services will continue to work.
- You must copy the `osso.conf` files generated during the upgrade, manually for each `OHS/mod_osso` fronting a set of partner applications. This step associates these applications with Oracle Access Manager 11.1.1.7.0 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 upgrade, Oracle Internet Directory is selected as the user identity store automatically.

Figure 3–4 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 C/ 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 upgrade scenario, follow the steps listed in Table 3–1.

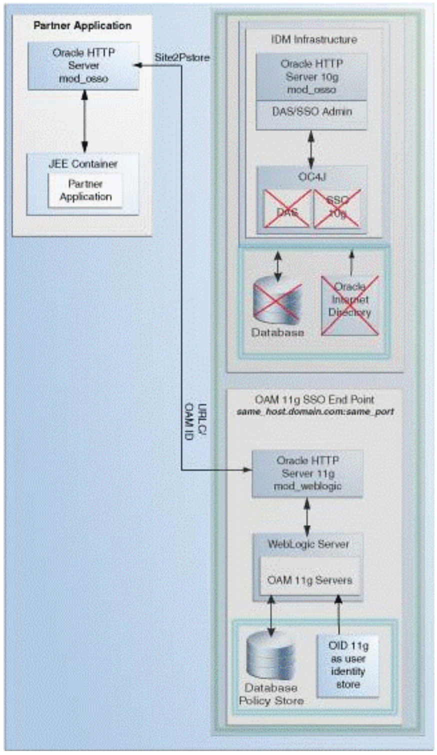
3.4.3 Oracle Delegated Administration Services Not Required After Upgrading Oracle Single Sign-On to Oracle Access Manager 11.1.1.7.0

Use this upgrade scenario if you do not require the Oracle Delegated Administration Services application or the Oracle Single Sign-On Admin tool. Figure 3–5 illustrates the scenario.

Note the following points when using this upgrade scenario:

- Oracle Single Sign-On and Oracle Delegated Administration Services will no longer work after the upgrade.
- Upgrade all the 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 Oracle Access Manager 11.1.1.7.0. 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 upgrade, Oracle Internet Directory is selected as the user identity store automatically.

Figure 3–5 Oracle Delegated Administration Services Not Required



To use this upgrade scenario, follow the steps listed in Table 3–1.

3.5 Upgrade Roadmap

Table 3–1 describes the tasks that should be completed for each of the Oracle Single Sign-On 10*g* upgrade scenarios.

Table 3–1 Upgrade Scenarios and Tasks

Scenario	Tasks to be Completed
Oracle Delegated Administration Services Required After Upgrading Oracle Single Sign-On 10*g* to Oracle Access Manager 11.1.1.7.0	▪ Section 3.6, "Prerequisites for Upgrade" ▪ Section 3.7, "Understanding the Oracle Access Manager 11.1.1.7.0 Topology" ▪ Section 3.8, "Optional: Upgrading the Oracle Database" ▪ Section 3.9, "Creating Schemas Using Repository Creation Utility" ▪ Section 3.10.1, "Installing and Configuring Oracle Access Manager 11.1.1.7.0 Using Oracle Single Sign-On 10g Host Name and Port Number" ▪ Section 3.11, "Upgrading Oracle Access Manager 11.1.1.7.0 Middle Tier Using Upgrade Assistant" ▪ Section 3.12, "Post-Upgrade Tasks" ▪ Section 3.13, "Verifying the Upgrade"
Oracle Delegated Administration Services Required, but Oracle Single Sign-On Admin Not Required After Upgrading Oracle Single Sign-On to Oracle Access Manager 11.1.1.7.0	▪ Section 3.6, "Prerequisites for Upgrade" ▪ Section 3.7, "Understanding the Oracle Access Manager 11.1.1.7.0 Topology" ▪ Section 3.8, "Optional: Upgrading the Oracle Database" ▪ Section 3.9, "Creating Schemas Using Repository Creation Utility" ▪ Section 3.10.2, "Installing and Configuring Oracle Access Manager 11.1.1.7.0 Using New Host Name or New Port Number" ▪ Section 3.11, "Upgrading Oracle Access Manager 11.1.1.7.0 Middle Tier Using Upgrade Assistant" ▪ Section 3.12, "Post-Upgrade Tasks" ▪ Section 3.13, "Verifying the Upgrade"
Oracle Delegated Administration Services Not Required After Upgrading Oracle Single Sign-On to Oracle Access Manager 11.1.1.7.0	▪ Section 3.6, "Prerequisites for Upgrade" ▪ Section 3.7, "Understanding the Oracle Access Manager 11.1.1.7.0 Topology" ▪ Section 3.8, "Optional: Upgrading the Oracle Database" ▪ Section 3.9, "Creating Schemas Using Repository Creation Utility" ▪ Section 3.10.1, "Installing and Configuring Oracle Access Manager 11.1.1.7.0 Using Oracle Single Sign-On 10g Host Name and Port Number" ▪ Section 3.11, "Upgrading Oracle Access Manager 11.1.1.7.0 Middle Tier Using Upgrade Assistant" ▪ Section 3.12, "Post-Upgrade Tasks" ▪ Section 3.13, "Verifying the Upgrade"

3.6 Prerequisites for Upgrade

You must complete the following prerequisites for upgrading Oracle Single Sign-On 10*g* to Oracle Access Manager 11.1.1.7.0:

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 upgrading.

   > **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 upgrade. For information about supported starting points for Oracle Single Sign-On 10*g* upgrade, see Section 2, "Upgrade Starting Points".

3.7 Understanding the Oracle Access Manager 11.1.1.7.0 Topology

Before you begin the upgrade process, get familiar with the topology of Oracle Access Manager 11.1.1.7.0.

For more information, see Section 3.3, "Topology Comparison".

3.8 Optional: Upgrading the Oracle Database

When you are upgrade an Oracle Single Sign-On environment to Oracle Access Manager 11.1.1.7.0, you must ensure that the version of the database where you plan to install the Oracle 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.

3.9 Creating Schemas Using Repository Creation Utility

You must create the necessary schemas in the database in order to configure Oracle Access Manager 11.1.1.7.0. 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 Oracle Access Manager 11.1.1.7.0, 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.*:

3.10 Installing and Configuring the Oracle Access Manager 11.1.1.7.0 Middle Tier

Depending on the upgrade scenario you choose, you must complete one of the following tasks:

- Installing and Configuring Oracle Access Manager 11.1.1.7.0 Using Oracle Single Sign-On 10g Host Name and Port Number

- Installing and Configuring Oracle Access Manager 11.1.1.7.0 Using New Host Name or New Port Number

3.10.1 Installing and Configuring Oracle Access Manager 11.1.1.7.0 Using Oracle Single Sign-On 10*g* Host Name and Port Number

Table 3–2 lists the steps to install and configure the Oracle Access Manager 11.1.1.7.0 middle tier for using the Oracle Delegated Administration Services application and the Oracle Single Sign-On Admin tool after upgrade from Oracle Single Sign-On 10*g* to Oracle Access Manager 11.1.1.7.0.

Table 3–2 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 WebLogic Server*.
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 11.1.1.7.0	See, "Installing and Configuring Oracle Identity and Access Management (11.1.1.7.0)" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.
5	Configuring Oracle Access Manager 11.1.1.7.0.	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 Oracle Access Manager 11.1.1.7.0 Managed Server with the Oracle HTTP Server 11g	See, Front-Ending Oracle Access Manager 11.1.1.7.0 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 Oracle Access Manager 11.1.1.7.0 Managed Server with Oracle HTTP Server 11*g*

You must use `mod_wl_ohs` to front-end Oracle Access Manager 11.1.1.7.0 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 Oracle Access Manager 11.1.1.7.0 Managed server. To restart the servers, you must first stop them, and then start.

For more information about starting and stopping the servers, see "Starting and Stopping Administration Servers" and "Starting and Stopping Oracle Fusion Middleware" 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 Oracle Access Manager 11.1.1.7.0. To do so, complete the following steps:

1. Log in to the Oracle Access Management 11.1.1.7.0 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
   ```

3.10.2 Installing and Configuring Oracle Access Manager 11.1.1.7.0 Using New Host Name or New Port Number

Table 3–3 lists the steps you must perform when installing and configuring the Oracle Access Manager 11.1.1.7.0 middle tier, using a new host name or port number for Oracle Access Manager.

Table 3–3 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 WebLogic Server*.
2	Installing Oracle Identity and Access Management 11*g* Release 1 (11.1.1.7.0)	See, "Installing and Configuring Oracle Identity and Access Management (11.1.1.7.0)" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.
3	Configuring Oracle Access Manager 11.1.1.7.0	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*.

3.11 Upgrading Oracle Access Manager 11.1.1.7.0 Middle Tier Using Upgrade Assistant

When you install Oracle Access Manager 11.1.1.7.0, 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 11.1.1.7.0 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 Oracle Access Manager 11.1.1.7.0 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**.

3.12 Post-Upgrade Tasks

The following sections describe the manual steps that you must perform after upgrading Oracle Single Sign-On 10*g* to Oracle Access Manager 11.1.1.7.0:

- Configuring Oracle Portal 10g with Oracle Access Manager 11.1.1.7.0 Server if the Oracle HTTP Server Port is Changed
- Configuring Oracle Access Manager 11.1.1.7.0 Administration Console to Align Roles
- Copying the osso.conf File
- Configuring Oracle Business Intelligence Discoverer 11g with Oracle Access Manager 11.1.1.7.0
- Setting the Headers in the Authentication Policy for the Protected DAS Resources
- Setting the Default Authentication Scheme
- Setting the Upgraded Identity Store as Default Store and System Store for Oracle Access Manager 11.1.1.7.0
- Additional Step for Oracle Internet Directory Configured in SSL Server Authentication Mode
- Additional Oracle Access Manager Post-Upgrade Tasks
- Decommissioning Oracle Single Sign-On 10g

3.12.1 Configuring Oracle Portal 10*g* with Oracle Access Manager 11.1.1.7.0 Server if the Oracle HTTP Server Port is Changed

After upgrading the Oracle Portal's Oracle Single Sign-On Server to the Oracle Access Manager 11.1.1.7.0 Server, you must update the Oracle Portal schema with information about the Oracle Access Manager 11.1.1.7.0 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 Oracle Access Manager 11.1.1.7.0 Managed Server host name and port number.

3.12.2 Configuring Oracle Access Manager 11.1.1.7.0 Administration Console to Align Roles

After upgrading, the Oracle Access Manager 11.1.1.7.0 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 Oracle Access Manager 11.1.1.7.0 Administrator for the Oracle Access Manager 11.1.1.7.0 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 Oracle Access Manager 11.1.1.7.0 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")
```

3.12.3 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 11.1.1.7.0.

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.

3.12.4 Configuring Oracle Business Intelligence Discoverer 11*g* with Oracle Access Manager 11.1.1.7.0

After upgrading the Oracle Business Intelligence Discoverer's Oracle Single Sign-On server to the Oracle Access Manager 11.1.1.7.0 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
```

3.12.5 Setting the Headers in the Authentication Policy for the Protected DAS Resources

After upgrading, you must set the headers in the authentication policy for protected Oracle Delegated Administration Services using the Oracle Access Management 11.1.1.7.0 console. To do this, complete the following steps:

1. Log in to the Oracle Access Manager 11.1.1.7.0 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 11.1.1.7.0 console
   - *port* refers to the designated bind port for the Oracle Access Manager 11.1.1.7.0 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 3–4 with the right values for **Name**, **Type**, and **Value** fields as specified in the table. Click **Add** after adding each header.

Table 3–4 Headers to be Added

Header Name	Type	Value
osso-subscriber	Header	*DEFAULT COMPANY*
osso-subscriber-dn	Header	*DN of subtree* For example: dc=us,dc=oracle,dc=com
osso-subscriber-guid	*Header*	*GUID for the DN*

3.12.6 Setting the Default Authentication Scheme

After upgrading, the default authentication scheme remains to be **LDAPScheme**. You must change this to **SSOCoexistMigrateScheme**. Therefore, after upgrading, you must set SSOCoexistMigrateScheme as the default authentication scheme using the Oracle Access Management 11.1.1.7.0 console. To do this, complete the following steps:

1. Log in to the Oracle Access Management 11.1.1.7.0 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 11.1.1.7.0 administration console
   - *port* refers to the designated bind port for the Oracle Access Management 11.1.1.7.0 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**.

3.12.7 Setting the Upgraded Identity Store as Default Store and System Store for Oracle Access Manager 11.1.1.7.0

After you upgrade Oracle Single Sign-On 10*g* to Oracle Access Manager 11.1.1.7.0, you must explicitly set the `migratedUserIdentityStore` as the Default Store and System Store for Oracle Access Manager 11.1.1.7.0. To do this, refer to "Setting the Default Store and System Store" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.

3.12.8 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 Oracle Access Manager 11.1.1.7.0 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>
   ```

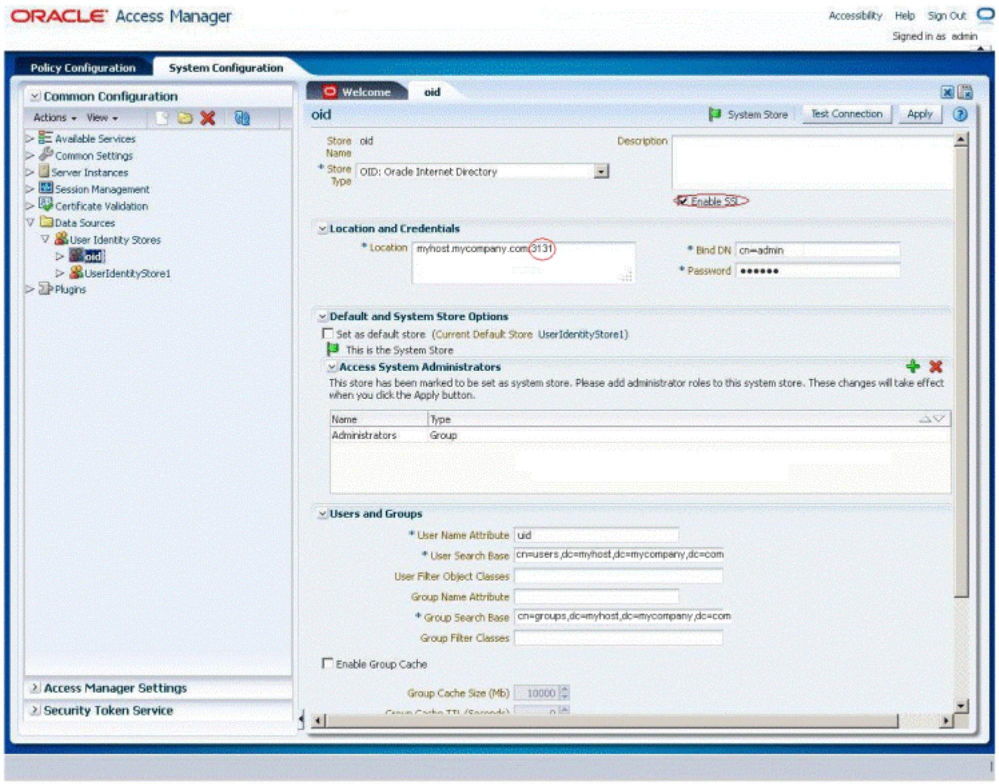
2. Restart the WebLogic Administration Server and the Oracle Access Manager 11.1.1.7.0 Managed Servers. To do this, follow Step-10 in Section 3.12.5, "Setting the Headers in the Authentication Policy for the Protected DAS Resources".
3. Log in to the Oracle Access Manager 11.1.1.7.0 console using the 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 3–6 shows the Oracle Access Manager console where you create new User Identity Store.

Figure 3–6 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

3.12.9 Additional Oracle Access Manager Post-Upgrade Tasks

You must perform the following additional post-upgrade tasks after upgrading to Oracle Access Manager 11.1.1.7.0:

- 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 upgrade 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 upgraded 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 Oracle Access Manager 11.1.1.7.0 for Single Sign-On authentication.

- In all other cases, the post-upgrade step of re-associating `mod_osso` partners with the newly upgraded Oracle Access Manager 11.1.1.7.0 is required. The `mod_osso` configurations generated as part of the upgrade 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
  ```

3.12.10 Decommissioning Oracle Single Sign-On 10*g*

After upgrading to Oracle Access Manager 11.1.1.7.0, 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
```

3.13 Verifying the Upgrade

After the upgrade is complete, the Oracle Access Manager will be in the co-existence mode, by default. To verify that your Oracle Access Manager upgrade 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 Oracle Access Manager 11.1.1.7.0 Administration Server is up and running, log in to the Oracle Access Management 11.1.1.7.0 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 Manager 11.1.1.7.0 administration console.
   - *`port`* refers to the designated bind port for the Oracle Access Manager 11.1.1.7.0 console, which is the same as the bind port for the Administration Server.

3. To verify that the Oracle Access Manager 11.1.1.7.0 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 upgrade log file for any error messages or use Fusion Middleware Control to verify that Oracle Access Manager 11.1.1.7.0 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*.

4 Upgrading Oracle Adaptive Access Manager 10*g* Environments

This chapter describes how to upgrade your existing Oracle Adaptive Access Manager 10*g* (10.1.4.5) to Oracle Adaptive Access Manager 11*g* Release 1 (11.1.1.7.0).

This chapter contains the following sections:

4.1 Overview

When you run Upgrade Assistant to upgrade from Oracle Adaptive Access Manager 10*g*, the Upgrade Assistant upgrades most of the Oracle Adaptive Access Manager 10*g* configuration to Oracle Adaptive Access Manager 11*g*. In some cases, you have to upgrade manually after you run the Upgrade Assistant.

When you run Upgrade Assistant to upgrade from Oracle Adaptive Access Manager 10*g*, the Upgrade Assistant upgrades the following:

- Symmetric keys (used for encryption and decryption) in the Adaptive Risk Manager Web Application (ARM) keystores, `system_config.keystore`, and `system_db.keystoreKeys` are migrated to the Credential Store Framework (CSF) with the same aliases under the credential map `oaam`.
- The following Oracle Adaptive Access Manager properties files of Authenticator Web Application (ASA):
  - `bharosauio.properties`
  - `bharosa_client.properties`
  - `bharosa_common.properties`
- The following Oracle Adaptive Access Manager properties files of Adaptive Risk Manager Web Application (ARM):
  - `bharosa_server.properties`
  - `bharosa_common.properties`

The following components are not upgraded to the Oracle Adaptive Access Manager 11*g* environment when you run Upgrade Assistant to upgrade from Oracle Adaptive Access Manager 10*g*:

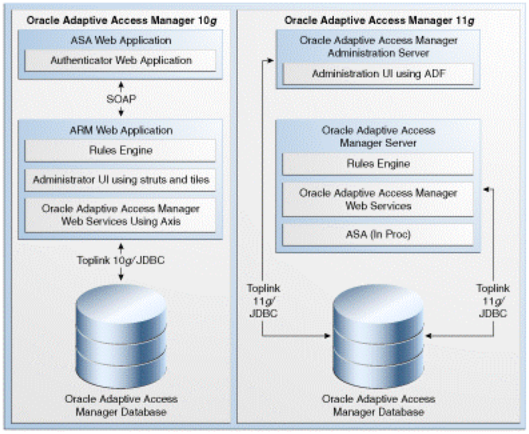
- ARM WebApp User Roles and Users
- `Log4j` settings
- Client-side Web Service configuration/settings in the ASA Web Application
- Client-side SOAP keystore with SOAP user password
- Any customizations, such as the following:
  - Custom Web Content (JSPs, CSS, etc)
  - Custom images
  - Custom Dynamic actions
  - Custom Loaders
  - Custom property files

You must upgrade such configuration manually after running Upgrade Assistant. For more information, see Task 11: Complete Any Required Oracle Adaptive Access Manager Post-Upgrade Tasks, *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*, and *Oracle Fusion Middleware Developer's Guide for Oracle Adaptive Access Manager*.

4.2 Topology Comparison

Table 4–1 compares a typical Oracle Adaptive Access Manager topology in Oracle Application Server 10g with a similar topology in Oracle Fusion Middleware 11g.

Figure 4–1 Comparison of Typical Oracle Adaptive Access Manager Topologies in Oracle Application Server 10g and Oracle Fusion Middleware 11g


Oracle Adaptive Access Manager 10*g*
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*g*
Oracle Adaptive Access Manager Administration Server
Administration UI using ADF
Oracle Adaptive Access Manager Server
Rules Engine
Oracle Adaptive Access Manager Web Services
ASA (In Proc)
Toplink 11*g*/ JDBC
Toplink 11*g*/ JDBC
Oracle Adaptive Access Manager Database

4.3 Task 1: Prerequisites

You must complete the following prerequisites for upgrading to the Oracle Adaptive Access Manager 11*g* environment:

- Ensure that you have applied the Bundle Patch 07 to the Oracle Adaptive Access Manager 10*g* (10.1.4.5) and to the Oracle Database.
- Ensure that your database meets the system requirements. For more information see *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*. If it does not meet the requirement, then you must upgrade the database software before upgrading to Oracle Adaptive Access Manager 11*g*.
- Make sure that the Oracle Adaptive Access Manager 10*g* web applications are in exploded format.
- Ensure that Oracle Adaptive Access Manager 10*g* `webapp` folders and files can be accessed by Upgrade Assistant.

4.4 Task 2: If Necessary, Upgrade the Oracle Database That Contains Oracle Adaptive Access Manager Schemas

If you are upgrading an Oracle Adaptive Access Manager environment, you must ensure that the version of the database where you plan to install the Oracle Adaptive Access Manager schemas is supported by Oracle Fusion Middleware 11*g*.

For instructions on verifying that your database meets the requirements of Oracle Fusion Middleware 11*g*, see "Upgrading and Preparing Your Databases" in the *Oracle Fusion Middleware Upgrade Planning Guide*.

4.5 Task 3: Run Repository Creation Utility to Create Schemas

Run the Repository Creation Utility to create the Oracle Meta Data Services (MDS) schema into a supported database and complete the following:

- Running Repository Creation Utility in Preparation for an Oracle Adaptive Access Manager Upgrade
- Selecting the Schemas Required for Oracle Adaptive Access Manager Upgrade

4.5.1 Running Repository Creation Utility in Preparation for an Oracle Adaptive Access Manager Upgrade

For information about running Repository Creation Utility to install the Oracle Adaptive Access Manager schema, refer to the following documents:

- *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*
- *Using Repository Creation Utility*

After you start the Repository Creation Utility, follow the instructions on the Repository Creation Utility screens to connect to the database and create the required schemas.

4.5.2 Selecting the Schemas Required for Oracle Adaptive Access Manager Upgrade

You can use Repository Creation Utility to install the schemas required for all of the Oracle Fusion Middleware software components that require a schema. However, there is no need to install all the schemas 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 Oracle Adaptive Access Manager upgrade, you must select the following schemas when prompted by the Repository Creation Utility:

- Expand **AS Common Schemas**, and select **Metadata Services** and **Audit Services**.

  This schema supports Oracle Fusion Middleware Metadata Services (MDS), which is required by the Oracle Adaptive Access Manager component.

> **Note:** The MDS Schema can be installed in a database other than the one where the Oracle Adaptive Access Manager schema is installed. However, ensure that the Oracle Adaptive Access Manager Managed Server can access your MDS schema.

4.6 Task 4: Install Oracle Fusion Middleware

Before you upgrade to Oracle Fusion Middleware 11g, you must install and configure an Oracle Fusion Middleware environment that is similar to the topology you set up for Oracle Application Server 10*g*. To do so, complete the following steps:

1. Installing Oracle WebLogic Server and Creating a Middleware Home
2. Installing Oracle Adaptive Access Manager 11g Release 1 (11.1.1.7.0)

4.6.1 Installing Oracle WebLogic Server and Creating a Middleware Home

Before you can install Oracle Identity and Access Management 11*g* Release 1 (11.1.1.7.0) components, you must install Oracle WebLogic Server and create the Oracle Middleware Home directory.

For more information, see "Install Oracle WebLogic Server" in *Oracle Fusion Middleware Installation Planning Guide for Oracle Identity and Access Management*.

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

4.6.2 Installing Oracle Adaptive Access Manager 11*g* Release 1 (11.1.1.7.0)

For information about installing Oracle Adaptive Access Manager 11*g* Release 1 (11.1.1.7.0), refer to "Installing and Configuring Oracle Identity and Access Management (11.1.1.7.0)" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

> **Note:** Do not configure the Oracle Adaptive Access Manager domain during the installation process.

4.7 Task 5: Use Upgrade Assistant to Upgrade the Oracle Adaptive Access Manager Schema

To upgrade the Oracle Adaptive Access Manager schema using Upgrade Assistant, perform the following steps:

1. Enter the following command to start the Upgrade Assistant:

   On UNIX systems (Located at *MW_HOME*/`Oracle_<IDM_Home>/bin`):

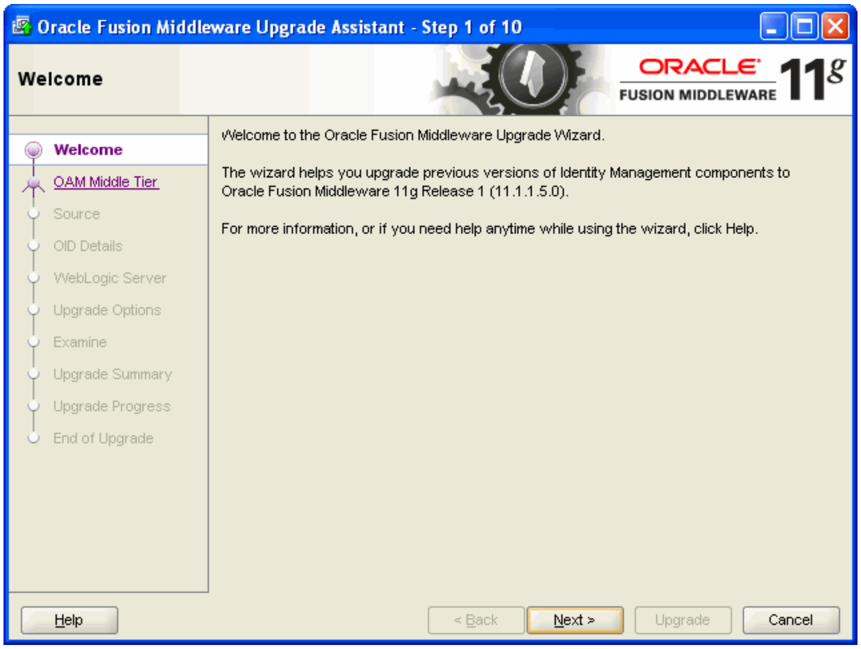
   ```
   ./ua
   ```

   On Windows systems (Located at *MW_HOME*`\Oracle_<IDM_Home>\bin`):

   ```
   ua.bat
   ```

   The Oracle Fusion Middleware Upgrade Assistant **Welcome** screen is displayed, as shown in Figure 4–2.

Figure 4–2 Upgrade Assistant Welcome Screen



Welcome to the Oracle Fusion Middleware Upgrade Wizard.

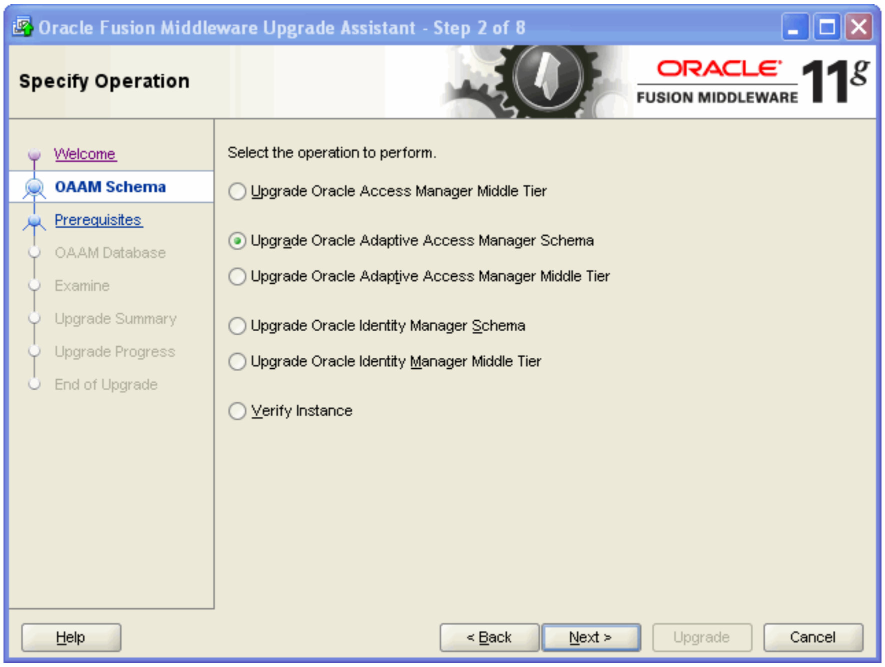
The wizard helps you upgrade previous versions of Identity Management components to Oracle Fusion Middleware 11g Release 1 (11.1.1.5.0).

For more information, or if you need help anytime while using the wizard, click Help.

2. Click **Next**.

   The **Specify Operation** screen is displayed, as shown in Figure 4–3.

Figure 4–3 Upgrade Assistant Specify Operation Screen



Select the operation to perform.

○ Upgrade Oracle Access Manager Middle Tier

● Upgrade Oracle Adaptive Access Manager Schema

○ Upgrade Oracle Adaptive Access Manager Middle Tier

○ Upgrade Oracle Identity Manager Schema

○ Upgrade Oracle Identity Manager Middle Tier

○ Verify Instance

3. Select the **Upgrade Oracle Adaptive Access Manager Schema** option.

4. Click **Next**.

   The **Prerequisites** screen is displayed.

5. Select the **Database Schema backup completed** and **Database version is certified by Oracle for Fusion Middleware upgrade** options.

   Note:

   - Ensure that the database has been upgraded before checking the **Database Schema backup completed** option. For more information, see Task 2: If Necessary, Upgrade the Oracle Database That Contains Oracle Adaptive Access Manager Schemas.

   - For instructions on verifying that your database meets the requirements of Oracle Fusion Middleware 11*g*, see `http://www.oracle.com/technology/software/products/ias/files/fusion_certification.html`.

   ---

6. Click **Next**.

   The **Specify OAAM Source Database** screen is displayed.

7. Enter the following information:

   - **Database Type**: Select the database type from the drop-down list.
   - **Connect String**: Enter the connect string for the database.

     For example:

     ```
     host:port:sid
     ```

- **OAAM Schema User**: Specify the Oracle Adaptive Access Manager 10*g* schema user name.
- **DBA User**: Enter the user name for your database.
- **DBA Password**: Enter the password for your database user.

8. Click **Next**.

   The **Examining Components** screen is displayed.

   Upgrade Assistant examines the components and checks that the source and target schemas contain the expected columns.

   Under the **Status** column, the word **succeeded** should appear. If instead, the word **failed** appears, inspect the log file for details.

   Note: If you want to view the log file for the current session, click on the link at the bottom of the screen to view the `ua.log` file.

9. Click **Next**.

   The **Upgrade Summary** screen is displayed.

10. Click **Upgrade**.

    The **Upgrade Progress** screen is displayed. This screen provides the following information:

    - Status of the upgrade
    - Any errors or problems that occur during the upgrade

    See Also: "Troubleshooting Your Upgrade" in the *Oracle Fusion Middleware Upgrade Planning Guide* for specific instructions for troubleshooting problems that occur while running the Upgrade Assistant

11. Click **Next**.

    The **Upgrade Complete** screen is displayed. This screen confirms that the upgrade was complete.

12. Click **Close**.

4.8 Task 6: Configure Oracle Adaptive Access Manager in a New or Existing Oracle WebLogic Domain

To configure Oracle Adaptive Access Manager in a new or existing Oracle WebLogic domain, refer to the "Configuring Oracle Adaptive Access Manager" section in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*. When you run the Oracle Fusion Middleware Configuration Wizard ensure that you configure the Managed Servers and assign them to machine.

> **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 will not be present in Oracle Adaptive Access Manager 10*g* database. You can ignore these errors and complete the Oracle Adaptive Access Manager 11*g* installation.

4.9 Task 7: Configure Node Manager to Start Managed Servers

For information about configuring Node Manager, refer to the "Configuring Node Manager to Start Managed Servers" section in the *Oracle Fusion Middleware Administrator's Guide*.

4.10 Task 8: Stop the Administration Server and Oracle Adaptive Access Manager Managed Servers

If you have started the Oracle Adaptive Access Manager Administration Server and the Oracle Adaptive Access Manager Managed Servers, then you must stop the Oracle Adaptive Access Manager Administration Server and Managed Servers by running the following command on the command line:

Windows

```
stopManagedWebLogic.cmd oaam_admin_server1
stopManagedWebLogic.cmd oaam_server_server1
```

UNIX

```
stopManagedWebLogic.sh oaam_admin_server1
stopManagedWebLogic.sh oaam_server_server1
```

4.11 Task 9: Use Upgrade Assistant to Upgrade Oracle Adaptive Access Manager Middle Tier

To upgrade the Oracle Adaptive Access Manager middle tier:

> **Note:** You can also use the Upgrade Assistant command-line interface to upgrade your Oracle Application Server 10*g* Oracle homes. For more information, see "Using the Upgrade Assistant Command-Line Interface" in the *Oracle Fusion Middleware Upgrade Planning Guide*.

1. If you have started the Oracle Adaptive Access Manager Managed Servers, then they will auto-generate symmetric keys required for encryption or decryption. You must delete keys before performing middle tier upgrade. To do so, complete the following steps:

   a. Log in to Oracle Enterprise Manager.

   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 symmetric key related entries.

2. Run the following command to launch Upgrade Assistant:

   On UNIX systems (Located at *MW_HOME*/`Oracle_<IDM_Home>/bin`):

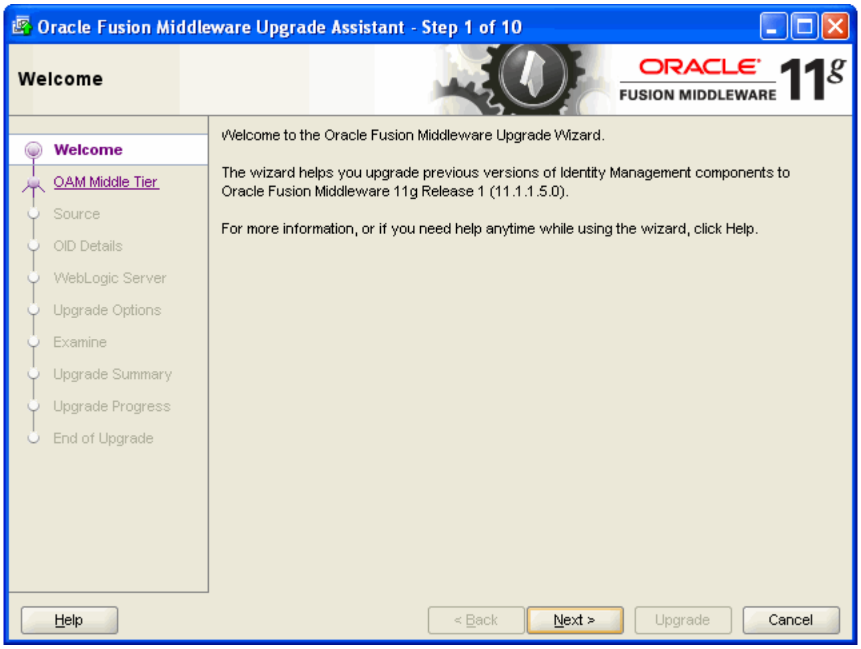
   ```
   ./ua
   ```

   On Windows systems (Located at *MW_HOME*\`Oracle_<IDM_Home>\bin`):

   ```
   ua.bat
   ```

   The Oracle Fusion Middleware Upgrade Assistant **Welcome** screen is displayed, as shown in Figure 4–4.

Figure 4–4 Upgrade Assistant Welcome Screen



Welcome to the Oracle Fusion Middleware Upgrade Wizard.

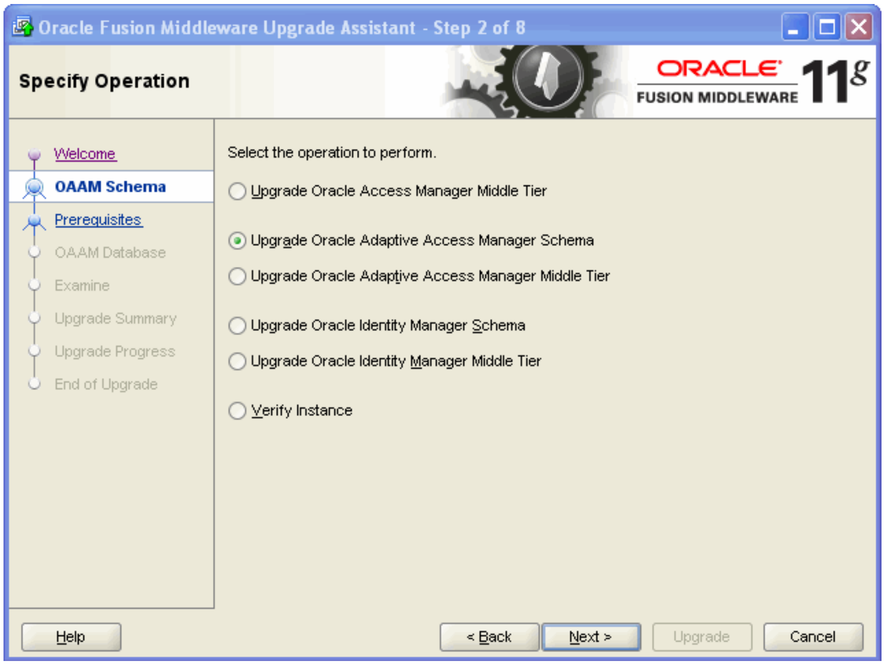
The wizard helps you upgrade previous versions of Identity Management components to Oracle Fusion Middleware 11g Release 1 (11.1.1.5.0).

For more information, or if you need help anytime while using the wizard, click Help.

3. Click **Next**.

   The **Specify Operation** screen is displayed, as shown in Figure 4–5.

Figure 4–5 Upgrade Assistant Specify Operation Screen



Select the operation to perform.

○ Upgrade Oracle Access Manager Middle Tier

● Upgrade Oracle Adaptive Access Manager Schema

○ Upgrade Oracle Adaptive Access Manager Middle Tier

○ Upgrade Oracle Identity Manager Schema

○ Upgrade Oracle Identity Manager Middle Tier

○ Verify Instance

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 format for Oracle Database:

     `//host:port/service` or `host:port:sid`
   - Schema User Name: Enter the user name for the schema.
   - Schema Password: Enter the password for the 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 Oracle WebLogic Server domain.
   - **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

    See Also: "Troubleshooting Your Upgrade" in the *Oracle Fusion Middleware Upgrade Planning Guide* for specific instructions for troubleshooting problems that occur while running the Upgrade Assistant.

12. Click **Next**.

    The **Upgrade Complete** screen is displayed. This screen confirms that the upgrade was complete.

13. Click **Close**.

4.12 Task 10: Start the Administration Server and Oracle Adaptive Access Manager Managed Servers

You must start the Oracle Adaptive Access Manager Administration Server and the Oracle Adaptive Access Manager Managed Servers by running the following command on the command line:

Windows

```
startManagedWebLogic.cmd oaam_admin_server1
startManagedWebLogic.cmd oaam_server_server1
```

UNIX

```
startManagedWebLogic.sh oaam_admin_server1
startManagedWebLogic.sh oaam_server_server1
```

4.13 Task 11: Complete Any Required Oracle Adaptive Access Manager Post-Upgrade Tasks

You must perform the following additional post-upgrade tasks after upgrading your Oracle Adaptive Access Manager 10*g* environment to Oracle Adaptive Access Manager 11*g*:

- If you have any customizations in Oracle Adaptive Access Manager 10*g*, then you can migrate these customizations using the customizations or extensions shared library for Oracle Adaptive Access Manager. For more information, see the *Oracle Fusion Middleware Developer's Guide for Oracle Adaptive Access Manager*.
- You must manually configure the Java logging setting because `log4j` is not used in Oracle Adaptive Access Manager 11*g*.
- Configure application logging using Oracle Fusion Middleware Enterprise Manager or configure the logging properties file that is used by the servers.
- You must reconfigure users with relevant Oracle Adaptive Access Manager groups in Oracle Adaptive Access Manager domain by using the Oracle WebLogic Administration console. These users can then use the `oaam_admin` application. The User Group roles used in Oracle Adaptive Access Manager 10*g* use a different set of names in Oracle Adaptive Access Manager 11*g*. Table 4–1 lists the role mapping from 10*g* to 11*g*.

Table 4–1 User Group Mapping

Oracle Adaptive Access Manager 10.1.4.5 User Group	Oracle Adaptive Access Manager 11G User Group
CSRGroup	OAAMCSRGroup
CSRManagerGroup	OAAMCSRManagerGroup
CSRInvestigator	OAAMCSRInvestigatorGroup
Investigator	OAAMInvestigatorGroup
InvestigationManager	OAAMInvestigationManagerGroup
RuleAdministratorsGroup	OAAMRuleAdministratorGroup
EnvAdminGroup	OAAMEnvAdminGroup
AuditorsGroup	Not Available
SOAPServicesGroup	OAAMSOAPServicesGroup

- Basic required entities are shipped along with Oracle Adaptive Access Manager in the `Auth_EntityDefinition.zip` file, which is located in the *`MW_HOME`*`/IDM_ORACLE_HOME/oaam/init` directory.You must import the basic entities into your system by completing the following steps:
  1. Log in to the Oracle Adaptive Access Manager Administration Console.
  2. Navigate to the Entities search page, by clicking **Entities** in the Navigation tree, or right-click **Entities** in the Navigation tree and select **Open** from the context menu that is displayed.
  3. In the Entities search page, click **Import**.
  4. In the Entities Import screen, click **Browse** and locate the `Auth_EntityDefinition.zip` file.
  5. Click **OK**.

- You must back-up the symmetric keys used for encryption and decryption. You may need this keys, if you have to recreate the Oracle Adaptive Access Manager 11*g* domain. Steps to access these keys

  a. Log in to Oracle Enterprise Manager.

  b. Expand the WebLogic Domain on the left pane, and select **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 select the symmetric key related entries associated with the Type **Generic**.

  e. Click **Edit**.

  f. Go to the **Credentials** section then copy the symmetric key related entries and note the key name.

  Note: Repeat the above steps to back-up database and configuration keys.

4.14 Task 12: Verify the Oracle Adaptive Access Manager Upgrade

To verify that your Oracle Adaptive Access Manager upgrade was successful:

1. Run Upgrade Assistant again, and select **Verify Instance** on the Specify Operation page.

   Follow the instructions on the screen for information about how to verify that specific Oracle Fusion Middleware components are up and running.

2. Use the following URL to verify that Oracle Adaptive Access Manager 11*g* is up and running:

   Oracle Adaptive Access Manager Administration Server:

   ```
   http://hostname:oaam_admin_port/oaam_admin/ping
   ```

   Oracle Adaptive Access Manager Managed Server:

   ```
   http://hostname:oaam_server_port/oaam_server/ping
   ```

   Alternatively, you can check the upgrade log file for any error messages or use Fusion Middleware Control to verify that Oracle Adaptive Access Manager 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*.

3. To verify that the Symmetric keys are created in CSF, perform the following:

   a. Log in to Oracle Enterprise Manager.

   b. Expand the WebLogic Domain on the left pane, and select **OAAM** domain.

      The OAAM domain page is displayed.

   c. From the OAAM Domain, select **Security**, and then **Credentials**.

      The **Credentials** page is displayed.

   d. Verify that **oaam** is listed in the **Credential Store Provider** table. Expand **oaam** and ensure that it includes the `DESede_db_key_alias` and `DESede_config_key_alias` entries.

4. Check the Oracle Adaptive Access Manager schema version, to ensure that the schema upgrade was successful.

5. Log in to the Oracle Adaptive Access Manager Administration Console as an existing user and ensure that you are able to access it.

6. To verify that you can search and view existing Sessions, perform the following:

   a. Log in to the Oracle Adaptive Access Manager Administration Console.

   b. In the Navigation tree, select **Sessions**. The Sessions search page is displayed.

   c. Search for the session by the details you are interested in.

   For more information, see the chapter "Using Session Details" in *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*.