Oracle® Fusion Middleware

Upgrade and Migration Guide for Oracle Identity and Access Management

11*g* Release 2 (11.1.2.1.0)

E28183-11

June 2014

Documentation for Oracle Fusion Middleware administrators who want to upgrade or migrate to Oracle Identity and Access Management 11*g* Release 2 (11.1.2.1.0).

ORACLE®

Oracle Fusion Middleware Upgrade and Migration Guide for Oracle Identity and Access Management, 11*g* Release 2 (11.1.2.1.0)

E28183-11

Primary Author: Shynitha K S

Contributors: Allison Sparshott, Arun Singla, Aruna Vempaty, Ashwini Singhvi, Ballaji Sahoo, Bhavik Sankesara, Brad Donnison, Bruce Xie, Charles Wesley, Deepak Ramakrishnan, Derick Leo, Gaurav Johar, 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, Sanjeev Sharma, Semyon Shulman, Sitaraman Swaminathan, Sree Chitturi, Srinivas Nagandla, Stephen Mathew, Steven Frehe, Stuart Duggan, Svetlana Kolomeyskaya, Tushar Wagh, Umesh Waghode, Vadim Lander, Vishal Mishra, Venu Shastri, William Cai, Wortimla Rs

Contents

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 Manager 9.x Environments

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

10 Migration and Coexistence Starting Points

11 Migrating Oracle Access Manager 10*g* Environments

12 Migrating Oracle Adaptive Access Manager 10*g* Environments

13 Migrating Oracle Single Sign-On 10*g* Environments

14 Migrating Sun OpenSSO Enterprise 8.0 Environments

16 Coexistence of Oracle Access Manager 10*g* with Oracle Access Management Access Manager 11.1.2.1.0

17 Coexistence of Sun OpenSSO Enterprise 8.0 with Oracle Access Management Access Manager 11.1.2.1.0

18 Coexistence of Sun Java System Access Manager 7.1 with Oracle Access Management Access Manager 11.1.2.1.0

Preface

This document describes how to upgrade or migrate to Oracle Identity and Access Management 11*g* Release 2 (11.1.2.1.0) components.

Audience

This document is intended for administrators who are responsible for upgrading or migrating to Oracle Identity and Access Management 11*g* Release 2 (11.1.2.1.0).

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 2 (11.1.2.1.0) 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*

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 (11.1.2.1.0) product. This chapters also describes the supported upgrade, migration, and coexistence scenarios for 11.1.2.1.0.

This chapter includes the following topics:

- Section 1.1, "Oracle Identity and Access Management Overview"
- Section 1.2, "Upgrade Scenarios"
- Section 1.3, "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 (11.1.2.1.0) 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 (11.1.2.1.0). For each of these upgrade scenarios, you use the Oracle Identity and Access Management 11*g* Release 2 (11.1.2.1.0) installer to update your existing Oracle Home (*IAM_HOME*) to Oracle Identity and Access Management 11*g* Release 2 (11.1.2.1.0).

You can upgrade the following Oracle Identity and Access Management components to Oracle Identity and Access Management 11.1.2.1.0:

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

> **Note:** Updating Oracle Identity and Access Management 11*g* Release 2 (11.1.2.0.0) environments to Oracle Identity and Access Management 11*g* Release 2 (11.1.2.1.0) involves applying patch as per Oracle Fusion Middleware standards. This procedure is covered in the *Oracle Fusion Middleware Patching Guide for Oracle Identity and Access Management*.
>
> For information about patching Oracle Identity and Access Management 11*g* Release 2 (11.1.2.0.0) to 11*g* Release 2 (11.1.2.1.0), see "Applying the Latest Oracle Fusion Middleware Patch Set" in the *Oracle Fusion Middleware Patching Guide for Oracle Identity and Access Management*.

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 (11.1.2.1.0). In these migration scenarios, you install a new 11*g* Release 2 (11.1.2.1.0) Oracle Home (*IAM_HOME*) and then migrate your configuration data from your previous installation to the new 11*g* Release 2 (11.1.2.1.0) 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 11.1.2.1.0 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 11.1.2.1.0 Servers.

The following are the coexistence scenarios supported in 11*g* Release 2 (11.1.2.1.0):

- Coexistence of Oracle Access Manager 10*g* with Oracle Access Management Access Manager 11.1.2.1.0
- Coexistence of Sun OpenSSO Enterprise 8.0 with Oracle Access Management Access Manager 11.1.2.1.0
- Coexistence of Sun Java System Access Manager 7.1 with Oracle Access Management Access Manager 11.1.2.1.0

2 Documentation Roadmap

This chapter describes the lists the upgrade, migration, and coexistence scenarios for Oracle Identity and Access Management 11*g* Release 2 (11.1.2.1.0).

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 11.1.2.1.0, and provides links to the chapters that describe each of the scenarios.

Table 2–1 Roadmap

Topic	Description
Upgrade Scenarios	See 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 8, "Upgrading Oracle Identity Navigator 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 9, "Upgrading Oracle Identity Manager 9.x Environments"
Migration Scenarios	See Chapter 11, "Migrating Oracle Access Manager 10g Environments" Chapter 12, "Migrating Oracle Adaptive Access Manager 10g Environments" Chapter 13, "Migrating Oracle Single Sign-On 10g Environments" Chapter 14, "Migrating Sun OpenSSO Enterprise 8.0 Environments" Chapter 15, "Migrating Sun Java System Access Manager 7.1 Environments"

Table 2–1 (Cont.) Roadmap

Topic	Description
Coexistence Scenarios	See, Chapter 16, "Coexistence of Oracle Access Manager 10g with Oracle Access Management Access Manager 11.1.2.1.0" Chapter 17, "Coexistence of Sun OpenSSO Enterprise 8.0 with Oracle Access Management Access Manager 11.1.2.1.0" Chapter 18, "Coexistence of Sun Java System Access Manager 7.1 with Oracle Access Management Access Manager 11.1.2.1.0"

Note: For information about patching Oracle Identity and Access Management 11*g* Release 2 (11.1.2.0.0) to 11*g* Release 2 (11.1.2.1.0), see "Applying the Latest Oracle Fusion Middleware Patch Set" in the *Oracle Fusion Middleware Patching Guide for Oracle Identity and Access Management*.

Part II

Upgrading Oracle Identity and Access Management 11.1.1.5.0 and 9.x 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 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:

- Section 3.1, "Supported Starting Points for Oracle Access Manager 11.1.1.5.0 Upgrade"
- Section 3.2, "Supported Starting Points for Oracle Adaptive Access Manager 11.1.1.5.0 Upgrade"
- Section 3.3, "Supported Starting Points for Oracle Identity Manager 11.1.1.5.0 Upgrade"
- Section 3.4, "Supported Starting Points for Oracle Entitlements Server 11.1.1.5.0 Upgrade"
- Section 3.5, "Supported Starting Points for Oracle Identity Manager 9.x Upgrade"

> **Note:** The patch sets listed in this chapter were 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,".

> **Note:** Updating Oracle Identity and Access Management 11*g* Release 2 (11.1.2.0.0) environments to Oracle Identity and Access Management 11*g* Release 2 (11.1.2.1.0) involves applying patch as per Oracle Fusion Middleware standards. This procedure is covered in the *Oracle Fusion Middleware Patching Guide for Oracle Identity and Access Management*.
>
> For information about patching Oracle Identity and Access Management 11*g* Release 2 (11.1.2.0.0) to 11*g* Release 2 (11.1.2.1.0), see "Applying the Latest Oracle Fusion Middleware Patch Set" in the *Oracle Fusion Middleware Patching Guide for Oracle Identity and Access Management*.

3.1 Supported Starting Points for Oracle Access Manager 11.1.1.5.0 Upgrade

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 (11.1.2.1.0):

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 ▪ Bundle Patch 11.1.1.5.2

3.2 Supported Starting Points for Oracle Adaptive Access Manager 11.1.1.5.0 Upgrade

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 (11.1.2.1.0):

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 ▪ Bundle Patch 11.1.1.5.2

3.3 Supported Starting Points for Oracle Identity Manager 11.1.1.5.0 Upgrade

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 (11.1.2.1.0):

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 Upgrade

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 (11.1.2.1.0):

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 Manager 9.x Upgrade

Table 3–5 lists the supported starting points for upgrading Oracle Identity Manager 9.x to Oracle Identity Manager 11*g* Release 2 (11.1.2.1.0):

Table 3–5 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 (11.1.2.1.0).

This chapter contains the following sections:

- Section 4.1, "Upgrade Roadmap for Oracle Access Manager"
- Section 4.2, "Upgrading Oracle Access Manager 11.1.1.5.0 to Oracle Access Management Access Manager 11.1.2"
- Section 4.3, "Updating Oracle Access Management Access Manager 11.1.2 to 11.1.2.1.0"

Before you 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.

4.1 Upgrade Roadmap for Oracle Access Manager

Table 4–1 lists the tasks to upgrade Oracle Access Manager 11.1.1.5.0 to Oracle Access Management Access Manager 11.1.2.1.0.

Table 4–1 Upgrade Flow

Task No.	Task	For More Information
1	Make sure that the Oracle Access Manager version you are using is supported for upgrade.	See, Supported Starting Points for Oracle Access Manager 11.1.1.5.0 Upgrade
2	Upgrade 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).	See, Upgrading Oracle Access Manager 11.1.1.5.0 to Oracle Access Management Access Manager 11.1.2
3	Update Oracle Access Management Access Manager 11g Release 2 (11.1.2) to 11*g* Release 2 (11.1.2.1.0).	See, Updating Oracle Access Management Access Manager 11.1.2 to 11.1.2.1.0

4.2 Upgrading Oracle Access Manager 11.1.1.5.0 to Oracle Access Management Access Manager 11.1.2

In order to upgrade Oracle Access Manager 11*g* Release 1 (11.1.1.5.0) to Oracle Access Management Access Manager 11*g* Release 2 (11.1.2.1.0), you must first upgrade Oracle Access Manager 11.1.1.5.0 to Oracle Access Management Access Manager 11.1.2.

For more information, see "Upgrading Oracle Access Manager 11*g* Release 1 (11.1.1.5.0) Environments" in the *Oracle Fusion Middleware Upgrade and Migration Guide for Oracle Identity and Access Management* for 11*g* Release 2 (11.1.2).

4.3 Updating Oracle Access Management Access Manager 11.1.2 to 11.1.2.1.0

To update Oracle Access Management Access Manager 11.1.2 to 11.1.2.1.0, follow the instructions described in the section "Applying the Latest Oracle Fusion Middleware Patch Set" in the *Oracle Fusion Middleware Patching Guide for Identity and Access Management*.

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 (11.1.2.1.0).

This chapter contains the following sections:

- Section 5.1, "Upgrade Roadmap for Oracle Adaptive Access Manager"
- Section 5.2, "Upgrading Oracle Adaptive Access Manager to Oracle Adaptive Access Manager 11.1.2"
- Section 5.3, "Updating Oracle Adaptive Access Manager 11.1.2 to 11.1.2.1.0"

Before you 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.

5.1 Upgrade Roadmap for Oracle Adaptive Access Manager

Table 5–1 lists the tasks to upgrade Oracle Adaptive Access Manager 11.1.1.5.0 to Oracle Adaptive Access Manager 11.1.2.1.0.

Table 5–1 Upgrade Flow

Task No.	Task	For More Information
1	Make sure that the Oracle Adaptive Access Manager version you are using is supported for upgrade.	See, Supported Starting Points for Oracle Adaptive Access Manager 11.1.1.5.0 Upgrade
2	Upgrade 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).	See, Upgrading Oracle Adaptive Access Manager to Oracle Adaptive Access Manager 11.1.2
3	Update Oracle Adaptive Access Manager 11g Release 2 (11.1.2) to 11*g* Release 2 (11.1.2.1.0).	See, Updating Oracle Adaptive Access Manager 11.1.2 to 11.1.2.1.0

5.2 Upgrading Oracle Adaptive Access Manager to Oracle Adaptive Access Manager 11.1.2

In order to upgrade Oracle Adaptive Access Manager 11*g* Release 1 (11.1.1.5.0) to Oracle Adaptive Access Manager 11*g* Release 2 (11.1.2.1.0), you must first upgrade Oracle Adaptive Access Manager 11.1.1.5.0 to Oracle Adaptive Access Manager 11.1.2.

For more information, see "Upgrading Oracle Adaptive Access Manager 11*g* Release 1 (11.1.1.5.0) Environments" in the *Oracle Fusion Middleware Upgrade and Migration Guide for Oracle Identity and Access Management* for 11*g* Release 2 (11.1.2).

5.3 Updating Oracle Adaptive Access Manager 11.1.2 to 11.1.2.1.0

To update Oracle Adaptive Access Manager 11.1.2 to 11.1.2.1.0, follow the instructions described in the section "Applying the Latest Oracle Fusion Middleware Patch Set" in the *Oracle Fusion Middleware Patching Guide for Identity and Access Management*.

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 (11.1.2.1.0).

This chapter contains the following sections:

- Section 6.1, "Upgrade Roadmap for Oracle Identity Manager"
- Section 6.2, "Upgrading Oracle Identity Manager 11.1.1.5.0 to Oracle Identity Manager 11.1.2.0.0"
- Section 6.3, "Updating Oracle Identity Manager 11.1.2.0.0 to 11.1.2.1.0"
- Section 6.4, "Performing Post-Upgrade Tasks"

Before you 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.

6.1 Upgrade Roadmap for Oracle Identity Manager

Table 6–1 lists the tasks to upgrade Oracle Identity Manager 11.1.1.5.0 to Oracle Identity Manager 11.1.2.1.0.

Table 6–1 Upgrade Flow

Task No.	Task	For More Information
1	Make sure that the Oracle Identity Manager version you are using is supported for upgrade.	See, Supported Starting Points for Oracle Identity Manager 11.1.1.5.0 Upgrade
2	Upgrade Oracle Identity Manager 11*g* Release 1 (11.1.1.5.0) to Oracle Identity Manager 11*g* Release 2 (11.1.2.0.0).	See, Upgrading Oracle Identity Manager 11.1.1.5.0 to Oracle Identity Manager 11.1.2.0.0
3	Update Oracle Identity Manager 11g Release 2 (11.1.2.0.0) to 11*g* Release 2 (11.1.2.1.0).	See, Updating Oracle Identity Manager 11.1.2.0.0 to 11.1.2.1.0
4	Perform the post upgrade tasks.	See, Performing Post-Upgrade Tasks

6.2 Upgrading Oracle Identity Manager 11.1.1.5.0 to Oracle Identity Manager 11.1.2.0.0

In order to upgrade Oracle Identity Manager 11*g* Release 1 (11.1.1.5.0) to Oracle Identity Manager 11*g* Release 2 (11.1.2.1.0), you must first upgrade Oracle Identity Manager 11.1.1.5.0 to Oracle Identity Manager 11.1.2.0.0.

For more information, see "Upgrading Oracle Identity Manager 11*g* Release 1 (11.1.1.5.0) Environments" in the *Oracle Fusion Middleware Upgrade and Migration Guide for Oracle Identity and Access Management* for 11*g* Release 2 (11.1.2).

> **Note:** When you upgrade Oracle Identity Manager 11.1.1.5.0 to Oracle Identity Manager 11.1.2.0.0, do NOT perform the post upgrade steps described in Section 6.4, "Post Upgrade Steps" in the *Oracle Fusion Middleware Upgrade and Migration Guide for Oracle Identity and Access Management* for 11*g* Release 2 (11.1.2).

6.3 Updating Oracle Identity Manager 11.1.2.0.0 to 11.1.2.1.0

To update Oracle Identity Manager 11*g* Release 2 (11.1.2.0.0) to Oracle Identity Manager 11*g* Release 2 (11.1.2.1.0), follow the instructions described in the section "Applying the Latest Oracle Fusion Middleware Patch Set" in the *Oracle Fusion Middleware Patching Guide for Identity and Access Management*.

6.4 Performing Post-Upgrade Tasks

After you upgrade Oracle Identity Manager 11.1.1.5.0 to Oracle Identity Manager 11.1.2.1.0, you must perform the post upgrade tasks described in Section 6.4, "Post Upgrade Tasks" in the *Oracle Fusion Middleware Upgrade and Migration Guide for Oracle Identity and Access Management* for 11*g* Release 2 (11.1.2).

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 (11.1.2.1.0).

This chapter contains the following sections:

- Section 7.1, "Upgrade Roadmap for Oracle Entitlements Server"
- Section 7.2, "Upgrading Oracle Entitlements Server 11.1.1.5.0 to Oracle Entitlements Server 11.1.2"
- Section 7.3, "Updating Oracle Entitlements Server 11.1.2 to 11.1.2.1.0"

Before you 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.

7.1 Upgrade Roadmap for Oracle Entitlements Server

Table 7–1 lists the tasks to upgrade Oracle Entitlements Server 11.1.1.5.0 to Oracle Entitlements Server 11.1.2.1.0.

Table 7–1 Upgrade Flow

Task No.	Task	For More Information
1	Make sure that the Oracle Entitlements Server version you are using is supported for upgrade.	See, Supported Starting Points for Oracle Entitlements Server 11.1.1.5.0 Upgrade
2	Upgrade Oracle Entitlements Server 11*g* Release 1 (11.1.1.5.0) to Oracle Entitlements Server 11*g* Release 2 (11.1.2).	See, Upgrading Oracle Entitlements Server 11.1.1.5.0 to Oracle Entitlements Server 11.1.2
3	Update Oracle Entitlements Server 11g Release 2 (11.1.2) to 11*g* Release 2 (11.1.2.1.0).	See, Updating Oracle Entitlements Server 11.1.2 to 11.1.2.1.0

7.2 Upgrading Oracle Entitlements Server 11.1.1.5.0 to Oracle Entitlements Server 11.1.2

In order to upgrade Oracle Entitlements Server 11*g* Release 1 (11.1.1.5.0) to Oracle Entitlements Server 11*g* Release 2 (11.1.2.1.0), you must first upgrade Oracle Entitlements Server 11.1.1.5.0 to Oracle Entitlements Server 11.1.2.

For more information, see "Upgrading Oracle Entitlements Server 11*g* Release 1 (11.1.1.5.0) Environments" in the *Oracle Fusion Middleware Upgrade and Migration Guide for Oracle Identity and Access Management* for 11*g* Release 2 (11.1.2).

7.3 Updating Oracle Entitlements Server 11.1.2 to 11.1.2.1.0

To update Oracle Entitlements Server 11.1.2 to 11.1.2.1.0, follow the instructions described in the section "Applying the Latest Oracle Fusion Middleware Patch Set" in the *Oracle Fusion Middleware Patching Guide for Identity and Access Management*.

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 (11.1.2.1.0).

This chapter includes the following sections:

Before you 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 11.1.2.1.0.	See, Upgrading Oracle Identity Navigator 11g Release 2 (11.1.2.1.0)
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 11.1.2.1.0 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 (11.1.2.1.0)

To upgrade Oracle Identity Navigator, you must use the Oracle Identity and Access Management 11.1.2.1.0 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 11.1.2.1.0.

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 (11.1.2.1.0)

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 (11.1.2.1.0)

Use Oracle Identity and Access Management 11.1.2.1.0 Installer to upgrade Oracle Identity Navigator 11.1.1.5.0 to Oracle Identity Navigator 11.1.2.1.0:

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 11.1.2.1.0 Oracle Identity and Access Management software to your system.

For more information, see "Installing and Configuring Oracle Identity and Access Management (11.1.2.1.0)" 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 11.1.2.1.0 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 opss-DBDS 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 11.1.2.1.0 installation. The following example shows the complete path: On UNIX, it is located in the `<MW_HOME>/user_projects/domains/base_domain/config/fmwconfig/jps-config.xml` directory. 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 11.1.2.1.0 installation. The following example shows the complete path: On UNIX, it is located in the `<MW_HOME>/oracle_common/modules/oracle.jps_11.1.1/domain_config/system-jazn-data.xml` directory. 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 11*g* Release 2 (11.1.2.1.0).

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 11.1.2.1.0.
>
> 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 11.1.2.1.0 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 11.1.2.1.0 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 11.1.2.1.0 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 11.1.2.1.0 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 11.1.2.1.0.

9 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 (11.1.2.1.0) which uses Oracle WebLogic Server as the application server.

> **Note:** If you wish to upgrade Oracle Identity Manager 9.x to Oracle Identity Manager 11*g* Release 2 (11.1.2.1.0) on IBM WebSphere, refer to *Oracle Fusion Middleware Third-Party Application Server Guide for Oracle Identity and Access Management*.

Upgrading Oracle Identity Manager 9.x to Oracle Identity Manager 11.1.2.1.0 involves three 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 (11.1.2.0.0)
- Updating Oracle Identity Manager 11*g* Release 2 (11.1.2.0.0) to Oracle Identity Manager 11*g* Release 2 (11.1.2.1.0)

The chapter contains the following sections:

- Section 9.1, "Overview"
- Section 9.2, "Upgrade Roadmap"
- Section 9.3, "Upgrading Oracle Identity Manager 9.x to Oracle Identity Manager 11.1.1.5.0"
- Section 9.4, "Upgrading Oracle Identity Manager 11.1.1.5.0 to Oracle Identity Manager 11.1.2.0.0"
- Section 9.5, "Updating Oracle Identity Manager 11.1.2.0.0 to Oracle Identity Manager 11.1.2.1.0"
- Section 9.6, "Performing Post-Upgrade Tasks"

Before you 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.

9.1 Overview

Before upgrading Oracle Identity Manager 9.x to Oracle Identity Manager 11.1.2.1.0, 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".

9.2 Upgrade Roadmap

Table 9–1 lists the steps to upgrade Oracle Identity Manager 9.x to Oracle Identity Manager 11.1.2.1.0.

Table 9–1 Upgrade Flow

Task No	Task	For More Information
1	Make sure that the Oracle Identity Manager 9.x version you are using is supported for upgrade.	See, Supported Starting Points for Oracle Identity Manager 9.x Upgrade
2	Upgrade your existing Oracle Identity Manager 9.x to Oracle Identity Manager 11.1.1.5.0.	See, Upgrading Oracle Identity Manager 9.x to Oracle Identity Manager 11.1.1.5.0
3	Upgrade Oracle Identity Manager 11.1.1.5.0 to Oracle Identity Manager 11.1.2.0.0	See, Upgrading Oracle Identity Manager 11.1.1.5.0 to Oracle Identity Manager 11.1.2.0.0
4	Update Oracle Identity Manager 11.1.2.0.0 to Oracle Identity Manager 11.1.2.1.0	See, Updating Oracle Identity Manager 11.1.2.0.0 to Oracle Identity Manager 11.1.2.1.0
5	Perform the post-upgrade tasks.	See, Performing Post-Upgrade Tasks

9.3 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*g* Release 1 (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.

> **Note:** When you upgrade Oracle Identity Manager 9.x to Oracle Identity Manager 11.1.1.5.0, do NOT perform the post-upgrade tasks described in Section 13.16, "Task 14: Complete Any Required Oracle Identity Manager Post-Upgrade Tasks" in the *Oracle Fusion Middleware Upgrade Guide for Oracle Identity Management* for 11*g* Release 1 (11.1.1).

9.4 Upgrading Oracle Identity Manager 11.1.1.5.0 to Oracle Identity Manager 11.1.2.0.0

To upgrade Oracle Identity Manager 11*g* Release 1 (11.1.1.5.0) to Oracle Identity Manager 11*g* Release 2 (11.1.2.0.0), refer to "Upgrading Oracle Identity Manager 11*g* Release 1 (11.1.1.5.0) Environments" in the *Oracle Fusion Middleware Upgrade and Migration Guide for Oracle Identity and Access Management* for 11*g* Release 2 (11.1.2).

Note: When you upgrade Oracle Identity Manager 11.1.1.5.0 to Oracle Identity Manager 11.1.2.0.0, do NOT perform the post-upgrade tasks described in Section 6.4, "Post Upgrade Steps" in the *Oracle Fusion Middleware Upgrade and Migration Guide for Oracle Identity and Access Management* for 11*g* Release 2 (11.1.2).

9.5 Updating Oracle Identity Manager 11.1.2.0.0 to Oracle Identity Manager 11.1.2.1.0

To update Oracle Identity Manager 11*g* Release 2 (11.1.2.0.0) to Oracle Identity Manager 11*g* Release 2 (11.1.2.1.0), see "Applying the Latest Oracle Fusion Middleware Patch Set" in the *Oracle Fusion Middleware Patching Guide for Identity and Access Management*.

9.6 Performing Post-Upgrade Tasks

After you upgrade Oracle Identity Manager 9.x to Oracle Identity Manager 11.1.2.1.0, you must perform the post-upgrade tasks described in the following sections:

1. Section 13.16, "Task 14: Complete Any Required Oracle Identity Manager Post-Upgrade Tasks" in the *Oracle Fusion Middleware Upgrade Guide for Oracle Identity Management* for 11*g* Release 1 (11.1.1).
2. Section 6.4, "Post Upgrade Steps" in the *Oracle Fusion Middleware Upgrade and Migration Guide for Oracle Identity and Access Management* for 11*g* Release 2 (11.1.2).

Part III

Migrating Various Oracle 10*g* and OpenSSO Environments

This part includes the following chapters:

10 Migration and Coexistence Starting Points

This chapter outlines the supported starting points for migration and coexistence scenarios.

The chapter contains the following sections:

- Section 10.1, "Supported Starting Points for Oracle Access Manager 10g Migration"
- Section 10.2, "Supported Starting Points for Oracle Adaptive Access Manager 10g Migration"
- Section 10.3, "Supported Starting Points for Oracle Single Sign-On 10g Migration"
- Section 10.4, "Supported Starting Points for Sun OpenSSO Enterprise Migration"
- Section 10.5, "Supported Starting Points for Sun Java System Access Manager Migration"
- Section 10.6, "Supported Starting Points for Coexistence of Oracle Access Manager 10g With Oracle Access Management Access Manager 11.1.2.1.0"
- Section 10.7, "Supported Starting Points for Coexistence of Sun OpenSSO Enterprise With Oracle Access Management Access Manager 11.1.2.1.0"
- Section 10.8, "Supported Starting Points for Coexistence of Sun Java System Access Manager With Oracle Access Management Access Manager 11.1.2.1.0"

> **Note:** The patch sets listed in this chapter were 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 about migration scenarios, see Section 1.3, "Migration and Coexistence Scenarios".

10.1 Supported Starting Points for Oracle Access Manager 10*g* Migration

Table 10–1 lists the releases of Oracle Access Manager 10*g* supported for migration.

Table 10–1 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.

10.2 Supported Starting Points for Oracle Adaptive Access Manager 10*g* Migration

Table 10–2 lists the releases of Oracle Adaptive Access Manager 10*g* supported for migration.

Table 10–2 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. Bundle Patch 13 Oracle Adaptive Access Manager 10*g* (10.1.4.5.2) is the latest patchset release for 10*g*.

10.3 Supported Starting Points for Oracle Single Sign-On 10*g* Migration

Table 10–3 lists the releases of Oracle Single Sign-On 10*g* supported for migration.

Table 10–3 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).

10.4 Supported Starting Points for Sun OpenSSO Enterprise Migration

Table 10–4 lists the releases of Sun OpenSSO Enterprise supported for migration.

Table 10–4 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.

10.5 Supported Starting Points for Sun Java System Access Manager Migration

Table 10–5 lists the releases of Sun Java System Access Manager supported for migration.

Table 10–5 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.

10.6 Supported Starting Points for Coexistence of Oracle Access Manager 10*g* With Oracle Access Management Access Manager 11.1.2.1.0

Table 10–6 lists the releases of Oracle Access Manager 10*g* supported for coexistence with Oracle Access Management Access Manager 11*g* Release 2 (11.1.2.1.0).

Table 10–6 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 (11.1.2.1.0) deployments coexist.

10.7 Supported Starting Points for Coexistence of Sun OpenSSO Enterprise With Oracle Access Management Access Manager 11.1.2.1.0

Table 10–7 lists the releases of Sun OpenSSO Enterprise supported for coexistence with Oracle Access Management Access Manager 11*g* Release 2 (11.1.2.1.0).

Table 10–7 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 (11.1.2.1.0) deployments coexist.

10.8 Supported Starting Points for Coexistence of Sun Java System Access Manager With Oracle Access Management Access Manager 11.1.2.1.0

Table 10–8 lists the releases of Sun Java System Access Manager supported for coexistence with Oracle Access Management Access Manager 11*g* Release 2 (11.1.2.1.0).

Table 10–8 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.

11

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 (11.1.2.1.0).

This chapter contains the following sections:

11.1 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 11.1.2.1.0.

- Host identifiers

- Agents
- Data stores
- Authentication schemes
- Resource types
- Policy domains

During this migration, you must install Access Manager 11*g* Release 2 (11.1.2.1.0), 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 (11.1.2.1.0) Oracle Home.

This section contains the following topics:

- Modes of Migration
- Migration Summary

11.1.1 Modes of Migration

The following are the three modes of migration that you can perform using the procedure described in this chapter:

- Complete Migration
- Incremental Migration
- Delta Migration

11.1.1.1 Complete Migration

This mode of migration migrates all artifacts of Oracle Access Manager 10*g*, which are compatible with 11.1.2.1.0, to Access Manager 11.1.2.1.0. You can perform complete migration only once. You can perform delta migration after performing complete migration, whereas incremental migration is not supported after complete migration.

11.1.1.2 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 11.1.2.1.0. 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 11.1.2.1.0 environment. If an artifact that you wish to migrate is already present in the Access Manager 11.1.2.1.0 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.

11.1.1.3 Delta Migration

Delta migration can be performed only after complete migration. Delta migration refers to the migration of changes (referred to as delta) that you make to the 10*g* artifacts after the complete migration.

When you perform delta migration, changes made in the policy domains are migrated along with their corresponding changes in the dependent artifacts. For example, after complete migration, if you add a new resource which uses a newly created host identifier, the next delta migration migrates the newly created host identifier first, and then the resource.

Newly added resource types and agents are not migrated as part of the delta migration. To migrate the resource types, you must associate them with any of the policy domains.

Delta migration migrates 'add' or 'modify' types of changes. This means that, if you add any new artifacts or modify any artifacts (except for resource types and agents) in the 10*g* deployment, you can migrate those changes using delta migration. Delta migration does not migrate the 'deletions', which means, if you delete any artifact in the 10*g* deployment, you cannot get the same artifact deleted in the 11*g* deployment using delta migration. Migration tool ensures that it maintains the integrity of the existing data in Access Manager 11*g* if it cannot migrate any particular changes.

You cannot perform complete migration or incremental migration after delta migration. However, you can perform delta migration multiple times.

> **Note:** Oracle Access Manager 10*g* to Access Manager 11.1.2.1.0 delta migration depends on the availability of the changes made to the Oracle Access Manager 10*g* deployment. Oracle Access Manager 10*g* keeps track of the changes made to the 10*g* deployment using `Sync Records`. `Sync Records` are created only if you select the check box **Update Cache** that is available on the policy administration webpage, when you modify any policy related artifact using the Oracle Access Manager 10*g* Policy Manager console.

11.1.2 Migration Summary

Table 11–1 summarizes the artifacts of Oracle Access Manager 10*g* that can be migrated to Access Manager 11.1.2.1.0:

Table 11–1 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 11.1.2.1.0. ▪ Host name variations in Oracle Access Manager 10*g*, which contain non-numeric characters in the port values, are not migrated to Access Manager 11.1.2.1.0. Such non-numeric port value is removed, and the host part of the variation is retained. ▪ 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.

Table 11–1 (Cont.) Compatibility of Artifacts

Artifact	Description
Agents	■ All attributes of the Oracle Access Manager 10*g* agent profile are supported in migration except for IIS impersonation user name and password. ■ 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 11.1.2.1.0 server depending to the security mode of the WebGates. For more information, see Section 11.7, "Configuring Transport Security Mode for Access Manager 11.1.2.1.0 Server". ■ 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 11–4. ■ 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 11.1.2.1.0 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 11.1.2.1.0. If the directory profile contains a secondary directory instance, it is migrated as a separate data store. ■ 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. ■ Migration of authentication schemes with customized authentication flows is also supported. ■ 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. ■ External authentication schemes from Oracle Access Manager 10*g* are not supported in Access Manager 11.1.2.1.0. Therefore, external authentication schemes are migrated to 11.1.2.1.0 using Delegated Authentication Protocol (DAP). The migrated scheme requires some post-migration steps. ■ Migration of custom authentication is not supported. If an authentication scheme contains custom plug-ins, such schemes may not be migrated correctly. ■ All authentication schemes of type **Anonymous** in Oracle Access Manager 10*g* are directly mapped to one single Authentication scheme **NONE** in Access Manager 11.1.2.1.0.
Resource Types	■ Oracle Access Manager 10*g* resource types and the migrated Access Manager 11.1.2.1.0 resources types have one-to-one mapping. ■ Resource types with name **HTTP**, **wl_authen** are not migrated, as they are available out-of-the-box in Access Manager 11.1.2.1.0.

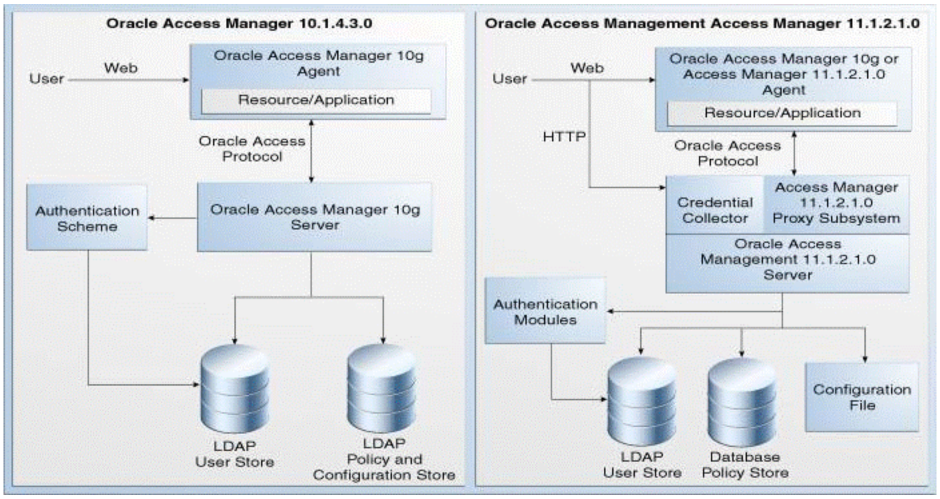
Table 11–1 (Cont.) Compatibility of Artifacts

Artifact	Description
Policy Domains	■ Policy domains of Oracle Access Manager 10*g* map to a distinct application domain in Access Manager 11.1.2.1.0. ■ URL prefixes are migrated to Access Manager 11.1.2.1.0. 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. ■ The default authentication rule and the authorization expression is migrated to the default authentication and authorization policy, respectively. ■ 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 11.1.2.1.0 does not support them. For authentication rules, both the success and failure redirects and responses are migrated to Access Manager 11.1.2.1.0. However, in the user interface, only success responses are displayed. ■ Authorization rules that do not form part of any authorization expression are ignored during migration. ■ While migrating Oracle Access Manager 10*g* internal policies to Access Manager 11.1.2.1.0: ■ 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. ■ 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. ■ 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. ■ Timing conditions are migrated as temporal conditions, and they form part of the ALLOW or DENY rule in Access Manager 11.1.2.1.0. ■ 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.

11.2 Topology Comparison

Figure 11–1 compares the topologies of Oracle Access Manager 10g and Access Manager 11.1.2.1.0.

Figure 11–1 Comparison of Oracle Access Manager 10g and Access Manager 11.1.2.1.0 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 11.1.2.1.0
User
Web
HTTP
Oracle Access Manager 10g or Access Manager 11.1.2.1.0 Agent
Resource/Application
Oracle Access Protocol
Credential Collector
Access Manager 11.1.2.1.0 Proxy Subsystem
Oracle Access Management 11.1.2.1.0 Server
Authentication Modules
Configuration File
LDAP User Store
Database Policy Store

11.3 Migration Roadmap

Table 11–2 lists the steps to migrate Oracle Access Manager 10*g* to Access Manager 11.1.2.1.0.

Table 11–2 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 (11.1.2.1.0).	See, Installing Oracle Identity and Access Management 11.1.2.1.0
3	Configure Access Manager 11.1.2.1.0.	See, Configuring Oracle Access Management Access Manager 11.1.2.1.0
4	Configure the security mode of the Access Manager 11.1.2.1.0 server instance and the WebGates, so that the Access Manager 11.1.2.1.0 server accepts connections from the agents when WebGates start communicating with Access Manager 11.1.2.1.0 after migration.	See, Configuring Transport Security Mode for Access Manager 11.1.2.1.0 Server

Table 11–2 (Cont.) Migration Tasks

Task No	Task	For More Information
5	Start the Administration Server and the Access Manager 11.1.2.1.0 Managed Servers.	See, Starting Administration Server and Access Manager 11.1.2.1.0 Managed Servers
6	Create a properties file with the LDAP details and the required information.	See, Creating the Properties File
7	Generate the assessment report, and analyze what agents and artifacts can be migrated to Access Manager 11.1.2.1.0. 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 11.1.2.1.0.	See, Restarting the Administration Server
9	If you wish to perform incremental migration, complete the additional steps (for example, creating an input file). 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 11.1.2.1.0.	See, Migrating the Artifacts of Oracle Access Manager 10g to Access Manager 11.1.2.1.0
11	If you are using 10*g* WebGates with Access Manager 11.1.2.1.0, you must configure the centralized logout for 10*g* WebGates to work with Access Manager 11.1.2.1.0 server.	See, Configuring Centralized Logout for 10g WebGates with Access Manager 11.1.2.1.0
12	Associate the migrated WebGates with the Oracle Access Management 11.1.2.1.0 Server.	See, Associating the WebGates with Access Manager 11.1.2.1.0 Server
13	Verify the migration.	See, Verifying the Migration

11.4 Prerequisites for Migration

You must complete the following prerequisites for migrating Oracle Access Manager 10*g* to Access Manager 11.1.2.1.0:

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 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 10.1, "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.

11.5 Installing Oracle Identity and Access Management 11.1.2.1.0

As part of the migration process, you must install Oracle Identity and Access Management 11*g* Release 2 (11.1.2.1.0). Oracle Identity and Access Management is a suite that contains Oracle Access Management Access Manager 11.1.2.1.0. 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 11.1.2.1.0, see "Installing Oracle Identity and Access Management (11.1.2.1.0)" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

11.6 Configuring Oracle Access Management Access Manager 11.1.2.1.0

After installing Oracle Identity and Access Management 11.1.2.1.0, you must configure Access Manager 11.1.2.1.0, and create a domain.

For information about configuring Access Manager 11.1.2.1.0, see "Configuring Oracle Access Management" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

11.7 Configuring Transport Security Mode for Access Manager 11.1.2.1.0 Server

You must configure the security mode of the Access Manager 11.1.2.1.0 Server, so that the migrated WebGates communicate with the Access Manager 11.1.2.1.0 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 11.1.2.1.0 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 11.1.2.1.0 Server
- Configuring Cert Mode Communication for Access Manager 11.1.2.1.0 Server
- Configuring Simple Mode Communication for Access Manager 11.1.2.1.0 Server

11.7.1 Deciding the Security Mode of Access Manager 11.1.2.1.0 Server

If all the WebGates that you migrate have the same security mode, you must configure the Access Manager 11.1.2.1.0 Server in the respective modes. If you have mix of migrated WebGates configured in different security modes, you must configure the Access Manager 11.1.2.1.0 Server in the mode with the lower security level. Table 11–3 lists the various use cases and the security mode in which you must configure the Access Manager 11.1.2.1.0 Server.

Table 11–3 Choosing the Security Mode for Access Manager 11.1.2.1.0 Server

Transport Security Mode of Oracle Access Manager 10*g* WebGates	Security Mode to be Configured for Access Manager 11.1.2.1.0 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 11.1.2.1.0 Server.
All Simple	Simple	See Configuring Simple Mode Communication for Access Manager 11.1.2.1.0 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 11.1.2.1.0 Server.

11.7.2 Configuring Cert Mode Communication for Access Manager 11.1.2.1.0 Server

To configure Cert mode communication for Access Manager 11.1.2.1.0, 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 11.1.2.1.0 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 11.1.2.1.0 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 11.1.2.1.0 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.

11.7.3 Configuring Simple Mode Communication for Access Manager 11.1.2.1.0 Server

To configure `Simple` mode communication for the Access Manager 11.1.2.1.0 Server, complete the following steps:

1. Log in to the Oracle Access Management 11.1.2.1.0 Administration console, using the following URL:

```
http://<host>:<port>/oamconsole
```

   where `<host>` is the machine on which Access Manager 11.1.2.1.0 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.

11.8 Starting Administration Server and Access Manager 11.1.2.1.0 Managed Servers

Before you start migrating Oracle Access Manager 10*g* to Access Manager 11.1.2.1.0, make sure that the WebLogic Administration Server and the Access Manager 11.1.2.1.0 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 11.1.2.1.0 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 11.1.2.1.0 Managed Servers

To start a Access Manager 11.1.2.1.0 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 11.1.2.1.0 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 11.1.2.1.0 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.

11.9 Creating the 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
## If the configuration store is SSL enabled, the LDAP url should begin with
'ldaps'.
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
## If the policy store is SSL enabled, the LDAP url should begin with 'ldaps'.
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

## This property indicates the path of trust store file which is a collective
## store of CA certs of all directory serves viz. policy store, config store,
## identity store.
ldap_trust_store=<path to ldap trust-store>

## This property is required if client authentication in directory
## server is enabled and it contains the path of file having client
```

```
## certificates
client_keystore=<path to ketstore file in jks format>

## If ldap_trust_store_password and client_keystore_password are left empty,
## then wlst commandline prompts for these passwords after migration utility
## is run.
ldap_trust_store_password=<plain text password of trust store file>
client_keystore_password=<plain text password of keystore file>

## 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: Incremental mode can be used to migrate selective artifacts
##                 from 10g enviroment. Incremental mode will be dictated by the
##                 include and exclude file properties. Incremental Migration
##                 cannot be performed after Complete Migration.
## 3. DELTA      : When the administrator intends to migrate the changes performed
to the 10g artifacts
##                 then delta migration can be performed. This will include all
the artifacts depending upon
##                 the GSN number.
## 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 11–4 describes the values you must provide for each of the properties in the properties file.

Table 11–4 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>` If the configuration store is SSL enabled, the LDAP URL should begin with '`ldaps`'.
`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: **1.** Log in to the Oracle Access Manager 10*g* Administration console. **2.** Go to the **System Configuration** tab. **3.** Click **Server settings** on the left navigation pane. **4.** Check for the value displayed for **Configuration Base**. Use the parent node of `oblix`. 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.

Table 11–4 (Cont.) Property File Values

Property	Description
`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: **1.** Move from your present working directory to the location: *Access_Server_Installation Directory*`/oblix/config/ldap/` **2.** Copy the value of `ldapRootPasswd` from the `ConfigDB.xml` file. **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>`. If the policy store is SSL enabled, the LDAP URL should begin with '`ldaps`'.
`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: **1.** Log in to the Oracle Access Manager 10*g* Administration console. **2.** Go to the **System Configuration** tab. **3.** Click **Server settings** on the left navigation pane. **4.** Check for the value displayed for **Policy Base**. Use the parent node of `oblix`. 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.
`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: **1.** Move from your present working directory to the location: *Access_Server_Installation_Directory*`/oblix/config/ldap/` **2.** Copy the value of `ldapRootPasswd` from the `WebResrcDB.xml` file. **3.** Use this value for the `policy_store_password` property in the properties file.
`policy_store_initial_context_factory`	The value of this property must be `com.sun.jndi.ldap.LdapCtxFactory`. Do not modify this value.
`ldap_trust_store`	Specify the path to the trust store file in `jks` format, which contains the CA certs of all SSL enabled directory servers.
`client_keystore`	Specify the path to the keystore file in `jks` format, which contains the client certificates. This property is required only if the client authentication is enabled. Otherwise, comment out this property using `#`.

Table 11–4 (Cont.) Property File Values

Property	Description
ldap_trust_store_password	Specify the plain text password for the trust store file that you specified for the property `ldap_trust_store`. If the value of this property is empty, the WLST command line prompts for password when you run the migration utility.
client_keystore_password	Specify the plain text password for the keystore file that you specified for the property `client_keystore`. This property is required only if you have specified the path of the keystore file for the `client_keystore` property. If the value of this property is empty, the WLST command line prompts for password when you run the migration utility.
migration_mode	This property indicates the mode of migration you wish to perform. Set one of the following values: ■ `COMPLETE` Specify this value if you wish to perform complete migration. This is ideal for a new Access Manager 11.1.2.1.0 environment with a clean database. ■ `INCREMENTAL` Specify this value if you wish to perform incremental migration. Incremental mode is dictated by the `include_file` and `exclude_file` properties that you specify in the properties file. ■ `DELTA` Specify this value if you wish to perform delta migration. 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 11.1.2.1.0, you must use the `include_file` property. 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 11.1.2.1.0. For more information about creating the include file, see "Additional Steps for Incremental Migration". If you wish to perform incremental migration with the `include_file` property, comment out the `exlcude_file` property. 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. For complete migration, this property is ignored.

Table 11–4 (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. 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 the exclude file, see "Additional Steps for Incremental Migration". If you wish to perform incremental migration with the exclude_file property, comment out the inlcude_file property. 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. 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. If the value of the preview_enabled property is set to false, the assessment report is not generated. 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: ■ COMPATIBLE ■ INCOMPATIBLE ■ ALL 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 11.1.2.1.0. 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 11.1.2.1.0, compatible with less features in Access Manager 11.1.2.1.0, and the artifacts that are ignored in Access Manager 11.1.2.1.0. 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 11.1.2.1.0, incompatible in Access Manager 11.1.2.1.0, compatible with less features in Access Manager 11.1.2.1.0, and the artifacts that are ignored in Access Manager 11.1.2.1.0. For more information about the artifacts that are incompatible, and compatible with less features, see Table 11–6.
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 11–4 (Cont.) Property File Values

Property	Description
evaluate_only	This properties indicates if the migration utility is run in evaluate mode. 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 11.1.2.1.0. 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 11.1.2.1.0. 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. If the amount of data that is migrated is more, and the memory is sufficient, set the value of this property to MAX. 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: ■ OPEN Specify this value if you wish to migrate all the agents in OPEN mode. ■ SIMpLE Specify this value if you wish to migrate all the agents in SIMPLE mode. ■ CERT Specify this value if you wish to migrate all the agents in CERT mode. ■ RETAIN_EXISTING Specify this value if you wish to migrate the agents in their existing modes. 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.

11.10 Generating the Assessment Report

You should generate an assessment report before you can migrate the Oracle Access Manager 10*g* artifacts to Access Manager 11.1.2.1.0.

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 11.1.2.1.0.

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 11.1.2.1.0
3. Detailed information about all the artifacts of Oracle Access Manager 10*g* in a tabular format.

Table 11–5 lists the columns of the table, which displays information about the artifacts of Oracle Access Manager 10*g*:

Table 11–5 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: ■ DATA SOURCES ■ AUTHENTICATION SCHEMES ■ RESOURCE TYPES ■ HOST IDs ■ AGENTS ■ POLICY DOMAINS
2	**ARTIFACT**	This column lists the names of all the artifacts of Oracle Access Manager 10*g*. 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. ■ For the artifact type **DATA SOURCES**, the name, host and port are listed here. ■ For the artifact type **AUTHENTICATION SCHEMES**, a description of each of the artifacts is displayed. ■ For the artifact type **RESOURCE TYPES**, the details of the artifact are displayed, if any. ■ For the artifacts type **HOST IDs**, the host and the port of each artifact is displayed. ■ For the artifacts type **AGENTS**, the mode of the artifact is displayed. ■ For the artifact type **POLICY DOMAINS**, the name of the policy domain is displayed.

Table 11–5 (Cont.) Assessment Report Content

Column No	Column	Description
4	**COMPATIBILITY**	This column displays information about the compatibility of artifacts in Access Manager 11.1.2.1.0.if the artifact is compatible with Access Manager 11.1.2.1.0 or not. The value for every artifact in this column can be one of the following: ■ **COMPATIBLE**: This indicates that the artifact is supported in Access Manager 11.1.2.1.0 and the migration utility does not perform any additional modelling. ■ **INCOMPATIBLE**: This indicates that the artifact is not supported in Access Manager 11.1.2.1.0, and will not be migrated. ■ **COMPATIBLE_WITH_LESS_FEATURES**: This indicates that the artifact is compatible in Access Manager 11.1.2.1.0, but with less features. The migration utility performs some modelling in order to map this artifact to 11.1.2.1.0. All the artifacts with this compatibility mode are migrated. ■ **IGNORE**: This indicates that the artifact is not useful in Access Manager 11.1.2.1.0, 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 11.1.2.1.0.

Table 11–6 shows the types of artifacts of Oracle Access Manager 10*g* that are incompatible and compatible with less features in Access Manager 11.1.2.1.0.

Table 11–6 Assessment Reports Summary

Artifacts	Description
INCOMPATIBLE	■ Policy domains that contain URL prefixes for heterogeneous resource types are incompatible with the Access Manager 11.1.2.1.0 environment. ■ Operation **OTHER** for type HTTP is incompatible with Access Manager 11.1.2.1.0, and is not migrated. ■ Delegated administration rights associated with policy domains are not considered for migration. ■ WebGate profile names greater than 255 characters are not migrated. ■ Authentication schemes containing custom authentication plug-ins are not migrated.

Table 11–6 (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. ■ Access Manager 11.1.2.1.0 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. ■ External authentication schemes such as DAP are not supported. ■ 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. ■ 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. ■ 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 11.1.2.1.0. The other conditions such as **Months of the Year** and **Days of the Month** are not supported in Access Manager 11.1.2.1.0, so they are not migrated. ■ 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 11.9, "Creating the 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 11.13, "Migrating the Artifacts of Oracle Access Manager 10g to Access Manager 11.1.2.1.0".

    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 11.13, "Migrating the Artifacts of Oracle Access Manager 10g to Access Manager 11.1.2.1.0".

> **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".

11.11 Restarting the Administration Server

Restart the WebLogic Administration Server for the domain with Access Manager 11.1.2.1.0 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.

11.12 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 11.9, "Creating the 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.

11.13 Migrating the Artifacts of Oracle Access Manager 10*g* to Access Manager 11.1.2.1.0

Before you migrate Oracle Access Manager 10*g* to Access Manager 11.1.2.1.0, it is recommended that you generate an assessment report (as described in Section 14.9, "Generating the Assessment Report"), and analyze what artifacts are compatible and incompatible in Access Manager 11.1.2.1.0.

> **Note:** If you decide to migrate Oracle Access Manager 10*g* to Access Manager 11.1.2.1.0 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 11.12, "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 the 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 11.1.2.1.0:

```
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 the Properties File. For example:

On UNIX:
```
oamMigrate(oamMigrateType="OAM10g",pathMigrationPropertiesFile="abc/def
/oam_migration.properties"
```

On Windows:
```
oamMigrate(oamMigrateType="OAM10g",pathMigrationPropertiesFile="abc\\de
f\\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.

11.14 Configuring Centralized Logout for 10*g* WebGates with Access Manager 11.1.2.1.0

If you are using 10*g* WebGates with Access Manager 11.1.2.1.0, you must configure the centralized logout settings for 10*g* WebGates to work with Access Manager 11.1.2.1.0 server, after migrating Oracle Access Manager 10*g* to Access Manager 11.1.2.1.0.

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 11.1.2.1.0.

11.15 Associating the WebGates with Access Manager 11.1.2.1.0 Server

After you migrate Oracle Access Manager 10*g* to Access Manager 11.1.2.1.0, you must associate all of the migrated WebGates with the Access Manager 11.1.2.1.0 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 11.1.2.1.0 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 11.1.2.1.0 Server instance is running.

      Port: Specify the proxy port for Access Manager 11.1.2.1.0 Server instance. The default proxy port for Access Manager 11.1.2.1.0 is `5575`.

      Transport Security: Specify the same transport security mode as that of the Access Manager 11.1.2.1.0 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 11.1.2.1.0 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 11.1.2.1.0 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 11.1.2.1.0 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 11.1.2.1.0 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 11.1.2.1.0 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 11.1.2.1.0 Server. If you restart the web server that hosts the WebGate, WebGate starts talking to the Access Manager 11.1.2.1.0 server immediately.

   - Increase the value of the parameter `MAX Connections` by one, so that the WebGate establishes the connection with Access Manager 11.1.2.1.0 server. If the load on WebGate is more, it takes less time to connect to the Access Manager 11.1.2.1.0 Server.

   WebGate now gets the new configuration information from the Access Manager 11.1.2.1.0 Server, which has only one primary server. Thus, the WebGate communicates only with the Access Manager 11.1.2.1.0 server. Once this is done, you can reduce the value of `MAX Connections` as there is only one server.

11.16 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 11.1.2.1.0 is running, and *`port`* is the port number.

   Verify that the Oracle Access Manager 10*g* artifacts are migrated to Access Manager 11.1.2.1.0.

Note: This completes the migration. For more information on managing the Oracle Access Management Access Manager 11.1.2.1.0, see *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.

11.17 Troubleshooting

This section describes solutions to the common problems that you might encounter when migration Oracle Access Manager 10*g* to Access Manager 11.1.2.1.0. 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

11.17.1 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**.

11.17.2 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
   ```

12

Migrating Oracle Adaptive Access Manager 10*g* Environments

This chapter describes how to migrate your existing Oracle Adaptive Access Manager (OAAM) 10*g* environment to Oracle Adaptive Access Manager 11*g* Release 2 (11.1.2.1.0).

This chapter contains the following sections:

12.1 Migration Overview

The process for migrating OAAM 10*g* to OAAM 11.1.2.1.0 involves two main tasks:

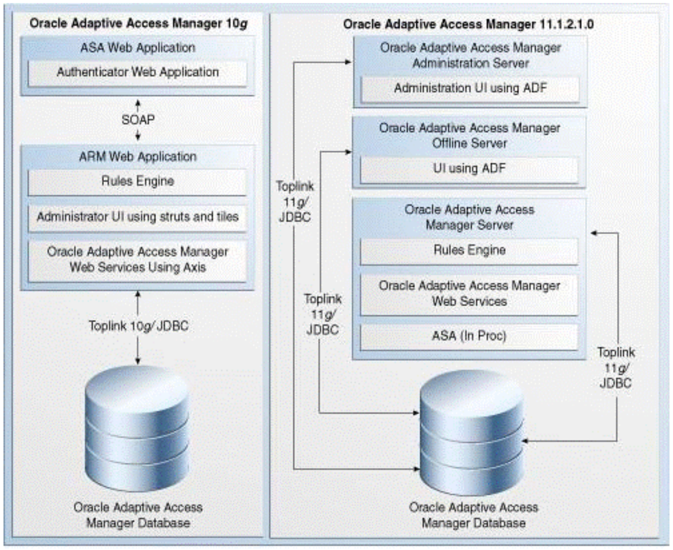
1. Upgrading OAAM 10*g* to OAAM 11*g* Release 2 (11.1.2)
2. Patching OAAM 11*g* Release 2 (11.1.2) to OAAM 11*g* Release 2 (11.1.2.1.0)

For more information about other migration scenarios, see Section 1.3, "Migration and Coexistence Scenarios".

12.2 Topology Comparison

Figure 12–1 compares the topologies of OAAM 10*g* and OAAM 11.1.2.1.0.

Figure 12–1 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 11.1.2.1.0
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

12.3 Migration Roadmap

Table 12–1 provides the migration roadmap.

Table 12–1 Task Roadmap

Task No	Task	For More Information
1	Upgrade OAAM 10*g* to OAAM 11.1.2.	See, Upgrading Oracle Adaptive Access Manager 10g to 11.1.2
2	Update OAAM 11.1.2 to OAAM 11.1.2.1.0.	See, Updating Oracle Access Management Access Manager 11.1.2 to 11.1.2.1.0

12.4 Upgrading Oracle Adaptive Access Manager 10*g* to 11.1.2

In order to upgrade OAAM 11*g* Release 1 (11.1.1.5.0) to OAAM 11*g* Release 2 (11.1.2.1.0), you must first upgrade OAAM 11.1.1.5.0 to OAAM 11*g* Release 2 (11.1.2).

For more information, see "Upgrading Oracle Adaptive Access Manager 10*g* Environments" in the *Oracle Fusion Middleware Upgrade and Migration Guide for Oracle Identity and Access Management* for 11*g* Release 2 (11.1.2).

12.5 Updating Oracle Access Management Access Manager 11.1.2 to 11.1.2.1.0

To update OAAM 11.1.2 to 11.1.2.1.0, see "Applying the Latest Oracle Fusion Middleware Patch Set" in the *Oracle Fusion Middleware Patching Guide for Identity and Access Management*.

13 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 (11.1.2.1.0).

This chapter contains the following sections:

13.1 Migration Overview

The process of migrating Oracle Single Sign-On 10*g* to Access Manager 11.1.2.1.0 involves installing Oracle Identity and Access Management 11.1.2.1.0, configuring Oracle Access Management Access Manager 11.1.2.1.0, and upgrading the Access Manager middle tier. Oracle Single Sign-On 10*g* to Access Manager 11.1.2.1.0 migration has three scenarios:

- Oracle Delegated Administration Services required after migrating Oracle Single Sign-On 10*g* to Access Manager 11.1.2.1.0

- Oracle Delegated Administration Services required, but Oracle Single Sign-On admin not required after migrating Oracle Single Sign-On 10*g* to Access Manager 11.1.2.1.0
- Oracle Delegated Administration Services not required after migrating Oracle Single Sign-On 10*g* to 11.1.2.1.0

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".

13.2 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

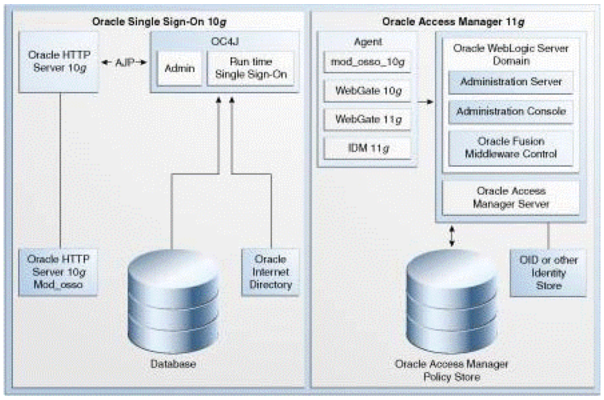
The following components are not migrated to Access Manager 11.1.2.1.0 environment when you run Upgrade Assistant to migrate from Oracle Single Sign-On 10*g*:

- 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.

13.3 Topology Comparison

Figure 13–1 compares a typical Oracle Single Sign-On topology in Oracle Application Server 10*g* with an Access Manager 11.1.2.1.0 topology in Oracle Fusion Middleware 11*g*.

Figure 13–1 Comparison of Typical Oracle Single Sign-On Topologies in Oracle Application Server 10g and Oracle Fusion Middleware 11g


Oracle Single Sign-On 10g
OC4J
Oracle HTTP Server 10g
AJP
Admin
Run time Single Sign-On
Oracle HTTP Server 10g Mod_osso
Oracle Internet Directory
Database
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

13.4 Migration Scenarios

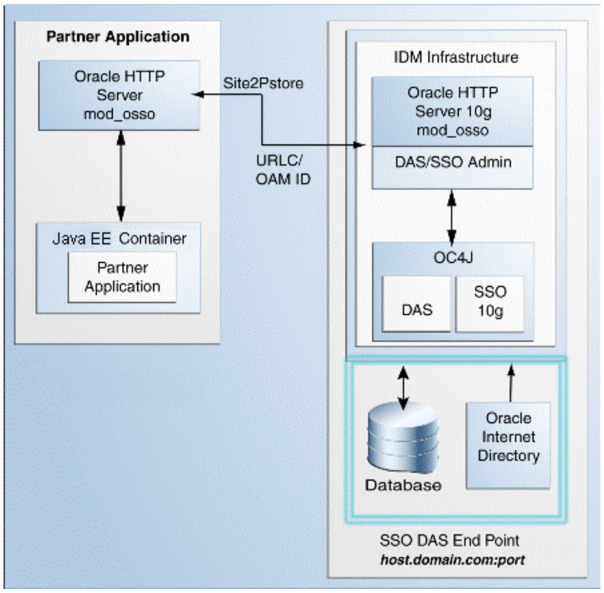
Before you migrate Oracle Single Sign-On 10*g* to Access Manager 11.1.2.1.0, you must consider your Oracle Single Sign-On 10*g* infrastructure (Figure 13–2) and depending on the functionality you choose to retain, you must select one of the following scenarios:

- Oracle Delegated Administration Services Required After Migrating Oracle Single Sign-On 10g to Access Manager 11.1.2.1.0
- Oracle Delegated Administration Services Required, but Oracle Single Sign-On Admin Not Required After Migrating Oracle Single Sign-On to Access Manager 11.1.2.1.0
- Oracle Delegated Administration Services Not Required After Migrating Oracle Single Sign-On to Access Manager 11.1.2.1.0

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

Figure 13–2 illustrates the Oracle Single Sign-On 10*g* topology.

Figure 13–2 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.

13.4.1 Oracle Delegated Administration Services Required After Migrating Oracle Single Sign-On 10*g* to Access Manager 11.1.2.1.0

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 11.1.2.1.0. Figure 13–3 illustrates the scenario.

Note the following points when using this migration scenario:

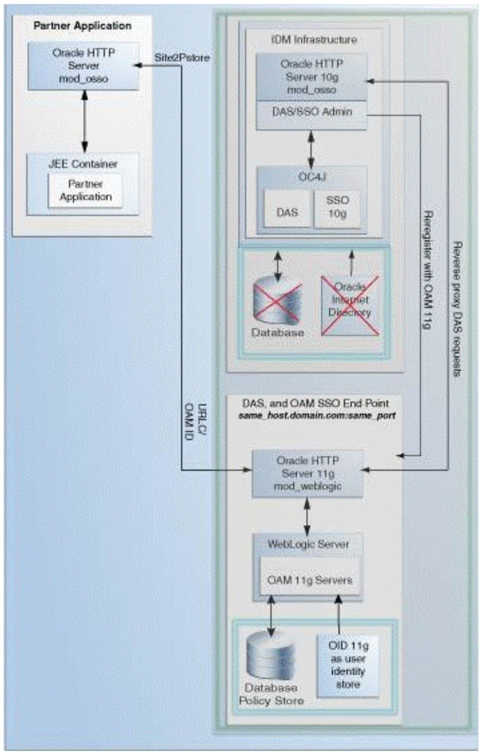
- Use this scenario if you are using Oracle Portal partner applications because you require Oracle Delegated Administration Services and Oracle Single Sign-On Administration. Migrate all partner applications at once.
- You are using the same Oracle HTTP Server 10*g* port that front-ended Oracle Single Sign-On 10*g* as the new port for Oracle Access Manager 11.1.2.1.0. Therefore, the Oracle Single Sign-On 10*g* server is no longer accessed. Instead, partner applications use Access Manager 11.1.2.1.0.

- 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 11.1.2.1.0 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 migration, Oracle Internet Directory is selected as the user identity store automatically.

Figure 13–3 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 13–1.

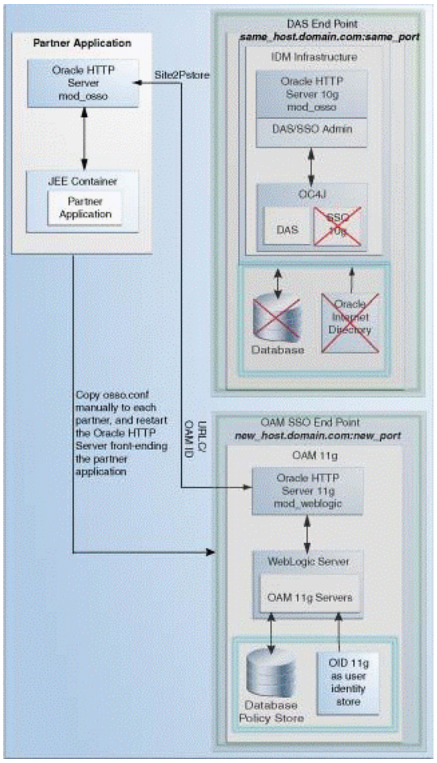
13.4.2 Oracle Delegated Administration Services Required, but Oracle Single Sign-On Admin Not Required After Migrating Oracle Single Sign-On to Access Manager 11.1.2.1.0

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 11.1.2.1.0. Figure 13–4 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 11.1.2.1.0 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 11.1.2.1.0 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 migration, Oracle Internet Directory is selected as the user identity store automatically.

Figure 13–4 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 migration scenario, follow the steps listed in Table 13–1.

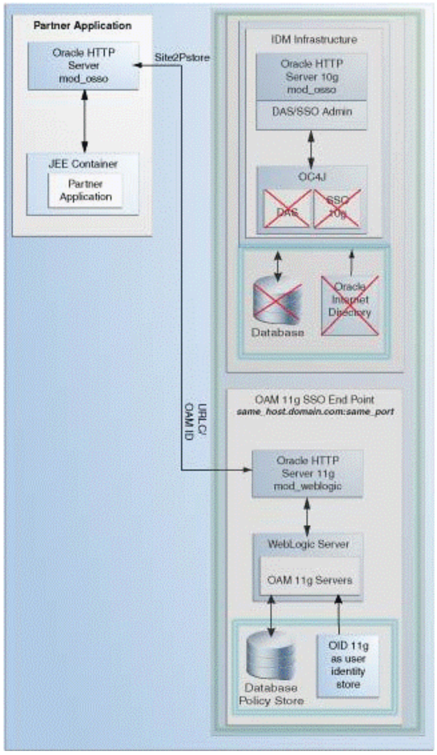
13.4.3 Oracle Delegated Administration Services Not Required After Migrating Oracle Single Sign-On to Access Manager 11.1.2.1.0

Use this migration scenario if you do not require the Oracle Delegated Administration Services application or the Oracle Single Sign-On Admin tool. Figure 13–5 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 11.1.2.1.0. 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 migration, Oracle Internet Directory is selected as the user identity store automatically.

Figure 13–5 Oracle Delegated Administration Services Not Required



To use this migration scenario, follow the steps listed in Table 13–1.

13.5 Migration Roadmap

Table 13–1 describes the tasks that should be completed for each of the Oracle Single Sign-On 10*g* migration scenarios.

Table 13–1 Migration Scenarios and Tasks

Scenario	Tasks to be Completed
Oracle Delegated Administration Services Required After Migrating Oracle Single Sign-On 10g to Access Manager 11.1.2.1.0	▪ Section 13.6, "Prerequisites for Migration" ▪ Section 13.7, "Understanding the Access Manager 11.1.2.1.0 Topology" ▪ Section 13.8, "Optional: Upgrading the Oracle Database" ▪ Section 13.9, "Creating Schemas Using Repository Creation Utility" ▪ Section 13.10.1, "Installing and Configuring Access Manager 11.1.2.1.0 Using Oracle Single Sign-On 10g Host Name and Port Number" ▪ Section 13.11, "Upgrading Access Manager 11.1.2.1.0 Middle Tier Using Upgrade Assistant" ▪ Section 13.12, "Performing Post-Migration Tasks" ▪ Section 13.13, "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 11.1.2.1.0	▪ Section 13.6, "Prerequisites for Migration" ▪ Section 13.7, "Understanding the Access Manager 11.1.2.1.0 Topology" ▪ Section 13.8, "Optional: Upgrading the Oracle Database" ▪ Section 13.9, "Creating Schemas Using Repository Creation Utility" ▪ Section 13.10.2, "Installing and Configuring Access Manager 11.1.2.1.0 Using New Host Name or New Port Number" ▪ Section 13.11, "Upgrading Access Manager 11.1.2.1.0 Middle Tier Using Upgrade Assistant" ▪ Section 13.12, "Performing Post-Migration Tasks" ▪ Section 13.13, "Verifying the Migration"
Oracle Delegated Administration Services Not Required After Migrating Oracle Single Sign-On to Access Manager 11.1.2.1.0	▪ Section 13.6, "Prerequisites for Migration" ▪ Section 13.7, "Understanding the Access Manager 11.1.2.1.0 Topology" ▪ Section 13.8, "Optional: Upgrading the Oracle Database" ▪ Section 13.9, "Creating Schemas Using Repository Creation Utility" ▪ Section 13.10.1, "Installing and Configuring Access Manager 11.1.2.1.0 Using Oracle Single Sign-On 10g Host Name and Port Number" ▪ Section 13.11, "Upgrading Access Manager 11.1.2.1.0 Middle Tier Using Upgrade Assistant" ▪ Section 13.12, "Performing Post-Migration Tasks" ▪ Section 13.13, "Verifying the Migration"

13.6 Prerequisites for Migration

You must complete the following prerequisites for migrating Oracle Single Sign-On 10*g* to Access Manager 11.1.2.1.0:

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 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 10.3, "Supported Starting Points for Oracle Single Sign-On 10g Migration".

13.7 Understanding the Access Manager 11.1.2.1.0 Topology

Before you begin the migration process, get familiar with the topology of Access Manager 11.1.2.1.0.

For more information, see Section 13.3, "Topology Comparison".

13.8 Optional: Upgrading the Oracle Database

When you are migrating an Oracle Single Sign-On environment to Access Manager 11.1.2.1.0, 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.

13.9 Creating Schemas Using Repository Creation Utility

You must create the necessary schemas in the database in order to configure Access Manager 11.1.2.1.0. 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 Access Manager 11.1.2.1.0, 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*.:

13.10 Installing and Configuring the Access Manager 11.1.2.1.0 Middle Tier

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

- Installing and Configuring Access Manager 11.1.2.1.0 Using Oracle Single Sign-On 10g Host Name and Port Number

- Installing and Configuring Access Manager 11.1.2.1.0 Using New Host Name or New Port Number

13.10.1 Installing and Configuring Access Manager 11.1.2.1.0 Using Oracle Single Sign-On 10*g* Host Name and Port Number

Table 13–2 lists the steps to install and configure the Access Manager 11.1.2.1.0 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 11.1.2.1.0.

Table 13–2 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 11.1.2.1.0	See, "Installing Oracle Identity and Access Management (11.1.2.1.0)" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.
5	Configuring Oracle Access Management Access Manager 11.1.2.1.0.	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 Access Manager 11.1.2.1.0 Managed Server with the Oracle HTTP Server 11g	See, Front-Ending Access Manager 11.1.2.1.0 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 Access Manager 11.1.2.1.0 Managed Server with Oracle HTTP Server 11*g*

You must use `mod_wl_ohs` to front-end Access Manager 11.1.2.1.0 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 Access Manager 11.1.2.1.0 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 Access Manager 11.1.2.1.0. To do so, complete the following steps:

1. Log in to the Oracle Access Management 11.1.2.1.0 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
```

13.10.2 Installing and Configuring Access Manager 11.1.2.1.0 Using New Host Name or New Port Number

Table 13–3 lists the steps you must perform when installing and configuring the Access Manager 11.1.2.1.0 middle tier, using a new host name or port number for Oracle Access Manager.

Table 13–3 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 (11.1.2.1.0)	See, "Installing Oracle Identity and Access Management (11.1.2.1.0)" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.
3	Configuring Oracle Access Management Access Manager 11.1.2.1.0	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*.

13.11 Upgrading Access Manager 11.1.2.1.0 Middle Tier Using Upgrade Assistant

When you install Access Manager 11.1.2.1.0, 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 11.1.2.1.0 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 Access Manager 11.1.2.1.0 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**.

13.12 Performing 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 11.1.2.1.0:

- Configuring Oracle Portal 10g with Access Manager 11.1.2.1.0 Server if the Oracle HTTP Server Port is Changed
- Configuring Oracle Access Management 11.1.2.1.0 Administration Console to Align Roles
- Copying the osso.conf File
- Configuring Oracle Business Intelligence Discoverer 11g with Access Manager 11.1.2.1.0
- 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 11.1.2.1.0
- Additional Step for Oracle Internet Directory Configured in SSL Server Authentication Mode
- Additional Access Manager Post-Migration Tasks
- Decommissioning Oracle Single Sign-On 10g

13.12.1 Configuring Oracle Portal 10*g* with Access Manager 11.1.2.1.0 Server if the Oracle HTTP Server Port is Changed

After migrating the Oracle Portal's Oracle Single Sign-On Server to the Access Manager 11.1.2.1.0 Server, you must update the Oracle Portal schema with information about the Access Manager 11.1.2.1.0 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 Access Manager 11.1.2.1.0 Managed Server host name and port number.

13.12.2 Configuring Oracle Access Management 11.1.2.1.0 Administration Console to Align Roles

After migration, the Oracle Access Management 11.1.2.1.0 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 Access Manager 11.1.2.1.0 Administrator for the Oracle Access Management 11.1.2.1.0 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 Access Manager 11.1.2.1.0 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")
```

13.12.3 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 11.1.2.1.0.

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.

13.12.4 Configuring Oracle Business Intelligence Discoverer 11*g* with Access Manager 11.1.2.1.0

After migrating the Oracle Business Intelligence Discoverer's Oracle Single Sign-On server to the Access Manager 11.1.2.1.0 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
```

13.12.5 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 11.1.2.1.0 console. To do this, complete the following steps:

1. Log in to the Oracle Access Management 11.1.2.1.0 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 11.1.2.1.0 console
- *port* refers to the designated bind port for the Oracle Access Management 11.1.2.1.0 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 13–4 with the right values for **Name**, **Type**, and **Value** fields as specified in the table. Click **Add** after adding each header.

Table 13–4 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*

10. Restart the WebLogic Administration Server and the Access Manager Managed Servers by completing the following tasks:

    a. Stop the WebLogic Administration Server by doing the following:

    On UNIX:

    Run the following commands:

    ```
    cd MW_HOME/user_projects/domains/domain_name/bin
    ./stopWebLogic.sh
    ```

    In this command, *MW_HOME* is the Middleware Home and *domain_name* is the name of the Access Manager domain.

    On Windows:

    Run the following commands:

    ```
    cd MW_HOME\user_projects\domains\domain_name\bin
    stopWebLogic.cmd
    ```

    In this command, *MW_HOME* is the Middleware Home and *domain_name* is the name of the Access Manager domain.

b. Stop the Access Manager Managed Servers by doing the following:

On UNIX:

Run the following commands:

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

```
./stopManagedWebLogic.sh managed_server_name admin_url user_name
password
```

In this command,

MW_HOME is the Middleware Home,

domain_name is the name of the Access Manager domain,

managed_server_name is the name of the Access Manager Managed Server,

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

user_name is the username of the WebLogic Administration Server,

password is the password of the WebLogic Administration Server.

On Windows:

Run the following commands:

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

```
stopManagedWebLogic.cmd managed_server_name admin_url user_name
password
```

In this command,

MW_HOME is the Middleware Home,

domain_name is the name of the Access Manager domain,

managed_server_name is the name of the Access Manager Managed Server,

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

user_name is the username of the WebLogic Administration Server,

password is the password of the WebLogic Administration Server.

c. Start the WebLogic Administration Server by doing the following:

On UNIX:

Run the following commands:

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

```
./startWebLogic.sh
```

In this command, *MW_HOME* is the Middleware Home and *domain_name* is the name of the Access Manager domain.

On Windows:

Run the following commands:

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

```
startWebLogic.cmd
```

In this command, *MW_HOME* is the Middleware Home and *domain_name* is the name of the Access Manager domain.

d. Start the Access Manager Managed Servers by doing the following:

On UNIX:

Run the following commands:

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

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

In this command,

MW_HOME is the Middleware Home,

domain_name is the name of the Access Manager domain,

managed_server_name is the name of the Access Manager Managed Server,

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

user_name is the username of the WebLogic Administration Server,

password is the password of the WebLogic Administration Server.

On Windows:

Run the following commands:

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

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

In this command,

MW_HOME is the Middleware Home,

domain_name is the name of the Access Manager domain,

managed_server_name is the name of the Access Manager Managed Server,

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

user_name is the username of the WebLogic Administration Server,

password is the password of the WebLogic Administration Server.

13.12.6 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 11.1.2.1.0 console. To do this, complete the following steps:

1. Log in to the Oracle Access Management 11.1.2.1.0 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 11.1.2.1.0 administration console
- *`port`* refers to the designated bind port for the Oracle Access Management 11.1.2.1.0 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**.

13.12.7 Setting the Migrated Identity Store as Default Store and System Store for Access Manager 11.1.2.1.0

After you migrate Oracle Single Sign-On 10*g* to Access Manager 11.1.2.1.0, you must explicitly set the `migratedUserIdentityStore` as the Default Store and System Store for Access Manager 11.1.2.1.0. To do this, refer to "Setting the Default Store and System Store" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.

13.12.8 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 Access Manager 11.1.2.1.0 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>
```

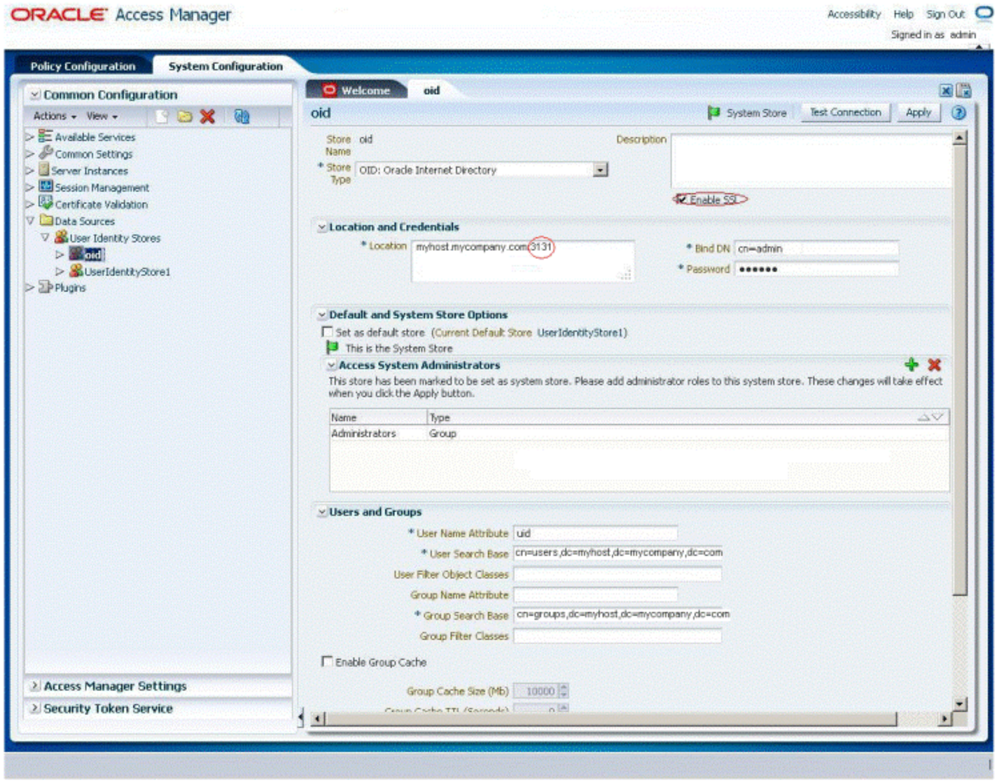
2. Restart the WebLogic Administration Server and the Access Manager 11.1.2.1.0 Managed Servers. To do this, follow Step-10 in Section 13.12.5, "Setting the Headers in the Authentication Policy for the Protected DAS Resources".
3. Log in to the Oracle Access Management 11.1.2.1.0 console using the following 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 13–6 shows the Access Manager console where you create new User Identity Store.

Figure 13–6 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

13.12.9 Additional Access Manager Post-Migration Tasks

You must perform the following additional post-migration tasks after migrating to Access Manager 11.1.2.1.0:

- 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 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 11.1.2.1.0 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 11.1.2.1.0 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
```

13.12.10 Decommissioning Oracle Single Sign-On 10*g*

After migrating to Access Manager 11.1.2.1.0, 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
```

13.13 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 11.1.2.1.0 Administration Server is up and running, log in to the Oracle Access Management 11.1.2.1.0 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 Management 11.1.2.1.0 administration console.
   - *port* refers to the designated bind port for the Oracle Access Management 11.1.2.1.0 console, which is the same as the bind port for the Administration Server.

3. To verify that the Access Manager 11.1.2.1.0 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 migration log file for any error messages or use Fusion Middleware Control to verify that Access Manager 11.1.2.1.0 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*.

14

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 (11.1.2.1.0).

The chapter contains the following sections:

14.1 Migration Overview

This section introduces two tools that are used in the process of migrating Sun OpenSSO Enterprise 8.0 to Oracle Access Manager 11.1.2.1.0.

OpenSSO Agent Assessment Tool

The OpenSSO Agent Assessment Tool reads the agents and policies from the OpenSSO Enterprise 8.0 server, analyzes the agents and the policy elements which can be migrated to Access Manager 11.1.2.1.0, 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 11.1.2.1.0 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 11.1.2.1.0, based on the understanding of the artifacts supported in Access Manager 11.1.2.1.0.

You can generate the assessment report more than once before you can migrate the OpenSSO Enterprise 8.0 to Access Manager 11.1.2.1.0.

Migration Tool

The Migration tool migrates the following artifacts of OpenSSO Enterprise 8.0 to Access Manager 11.1.2.1.0:

- 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".

14.2 Modes of Migration

This section describes the three modes of migration that you can perform using the procedure described in this chapter. The following are the two modes of migration:

- Complete Migration
- Incremental Migration
- Delta Migration

14.2.1 Complete Migration

Complete Migration migrates all compatible agents, policies, user stores, and authentication stores of OpenSSO Enterprise 8.0 to Access Manager 11.1.2.1.0. 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 11.1.2.1.0 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.

14.2.2 Incremental Migration

Incremental Migration is referred to as Selective Migration, as you can select the agents and polices of OpenSSO Enterprise 8.0 that you wish to migrate to Access Manager 11.1.2.1.0. You can perform this migration multiple times with different sets of agents and policies, and therefore it is called Incremental Migration. Selecting only the user stores or authentication stores for incremental migration is not supported. When you select the agents and policies for incremental migration, you must also select the respective user stores and authentication stores.

Note: You can perform Incremental Migration after performing Complete Migration, which will be referred to as Incremental Delta.

You can perform a Complete Migration after multiple Incremental Migration. In this case, the Complete Migration ignores the agents and policies that are already migration as part of the previous Incremental Migrations.

When you perform multiple Incremental Migrations by selecting the artifacts (agents and policies) that are already migrated, those artifacts are ignored, and the Incremental Migration migrates only the non-migrated artifacts.

14.2.3 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 11.1.2.1.0. 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 11.1.2.1.0 configuration store is retrieved, is incremented by one, and is saved back to the Access Manager 11.1.2.1.0 configuration store.

The procedure to perform a delta migration is same as that of a complete migration, and is described in Migration Roadmap.

14.3 Migration Summary

This sections summarizes the artifacts of OpenSSO Enterprise 8.0 that are compatible with Access Manager 11.1.2.1.0. 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

14.3.1 Summary of Migration of Agents

This section summarizes the migration of agents from OpenSSO Enterprise 8.0 to Access Manager 11.1.2.1.0.

- 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 11.1.2.1.0. 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 11.1.2.1.0.
- 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 11.1.2.1.0 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`.

14.3.2 Summary of Migration of Policies

This section summarizes the migration of policies from OpenSSO Enterprise 8.0 to Access Manager 11.1.2.1.0.

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 11.1.2.1.0:

- **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 11.1.2.1.0. All the auto policies can be migrated to Access Manager 11.1.2.1.0.
- **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 11.1.2.1.0. Semi policies are not migrated to Access Manager 11.1.2.1.0.
- **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 11.1.2.1.0. Manual policies are not migrated to Access Manager 11.1.2.1.0.

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 11.1.2.1.0) are not supported in Access Manager 11.1.2.1.0.

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 11.1.2.1.0.

Conditions

- Active Session Time
  - This condition of OpenSSO Enterprise policy is mapped to the attribute `Session Expiry Time` of the AttributeCondition in Access Manager 11.1.2.1.0.
  - The attribute `Terminate session` of this condition is ignored during migration as the appropriate mapping of this attribute does not exist in Access Manager 11.1.2.1.0.
- Authentication by Module Instance
  - This condition of OpenSSO Enterprise policy is migrated to Access Manager 11.1.2.1.0 as `AuthN` scheme, and not as a condition.
  - Table 14–1 lists the authentication modules of OpenSSO Enterprise 8.0 that are migrated and mapped with `AuthN` scheme into Access Manager 11.1.2.1.0.

Table 14–1 Mapping of Authentication Module

Authentication Module in OpenSSO Enterprise 8.0	Authentication Plug-in in Access Manager 11.1.2.1.0
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 11.1.2.1.0 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 11.1.2.1.0.

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 11.1.2.1.0 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 11.1.2.1.0 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 11.1.2.1.0.
  - 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 11.1.2.1.0.
  - 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 11.1.2.1.0.
  - The condition `DNS name` is not supported in Access Manager 11.1.2.1.0.
- LDAP Filter Condition
  - This condition in OpenSSO Enterprise policy is mapped to `Identity condition` in Access Manager 11.1.2.1.0.
  - 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 11.1.2.1.0.
- Time (day, date, time, and time zone)
  - This condition in OpenSSO Enterprise 8.0 policy is mapped to `Time condition` in Access Manager 11.1.2.1.0.
  - 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 11.1.2.1.0 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 11.1.2.1.0. 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 11.1.2.1.0 with the type Http header.

14.3.3 Summary of Migration of User Stores

This section summarizes the migration of user stores from OpenSSO Enterprise 8.0 to Access Manager 11.1.2.1.0.

OpenSSO Enterprise has three types of user stores:

- **Active Directory**: This user store can be migrated to Access Manager 11.1.2.1.0.
- **Generic LDAPv3**: This user store can be migrated to Access Manager 11.1.2.1.0.
- **Sun DS with OpenSSO schema**: This user store cannot be migrated to Access Manager 11.1.2.1.0, as no supported data store type is available in 11.1.2.1.0.

14.3.4 Summary of Migration of Authentication Stores

This section summarizes the migration of authentication stores from OpenSSO Enterprise 8.0 to Access Manager 11.1.2.1.0.

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 11.1.2.1.0:

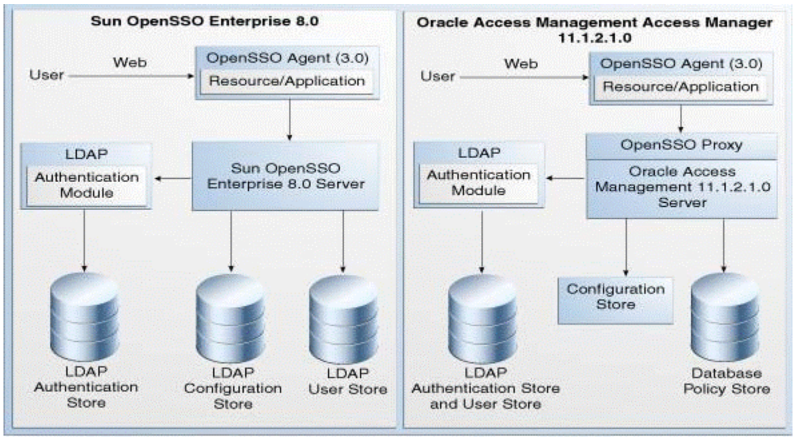
- LDAP in OpenSSO Enterprise 8.0 is mapped to OAM LDAP in Access Manager 11.1.2.1.0.
- Certificate in OpenSSO Enterprise 8.0 is mapped to X509 in Access Manager 11.1.2.1.0.
- Windows Desktop SSO in OpenSSO Enterprise 8.0 is mapped to Kerberos Access Manager 11.1.2.1.0.

All authentication stores with type LDAP are migrated to Access Manager 11.1.2.1.0 with name `AS_`*`RealmName`*`_`*`Modulename`*. The authentication stores with type other than LDAP are not migrated.

14.4 Topology Comparison

Figure 14–1 compares the topologies of Sun OpenSSO Enterprise 8.0 and Access Manager 11.1.2.1.0.

Figure 14–1 OpenSSO Enterprise 8.0 and Access Manager 11.1.2.1.0 Topologies



14.5 Migration Roadmap

Table 14–2 lists the steps to migrate Sun OpenSSO Enterprise 8.0 to Access Manager 11.1.2.1.0.

Table 14–2 Task Roadmap

Task No	Task	For More Information
1	Complete the prerequisites.	See, Prerequisites for Migration
2	Install Oracle Identity and Access Management 11.1.2.1.0.	See, Installing Oracle Identity and Access Management 11.1.2.1.0
3	Configure Oracle Access Management Access Manager 11.1.2.1.0.	See, Configuring Oracle Access Management Access Manager 11.1.2.1.0
4	Generate the assessment report, and analyze what artifacts can be migrated to Access Manager 11.1.2.1.0. You can perform this task multiple times.	See, Generating the Assessment Report
5	Start the WebLogic Administration Server.	See, Starting the WebLogic Administration Server
6	If you wish to perform Incremental Migration, complete the additional steps.	See, Additional Steps for Incremental Migration
7	Create the properties file.	See, Creating the Properties File
8	Migrate OpenSSO Enterprise 8.0 to Access Manager 11.1.2.1.0 by running the migration tool.	See, Migrating the Artifacts of OpenSSO Enterprise 8.0 to Access Manager 11.1.2.1.0

Table 14–2 (Cont.) Task Roadmap

Task No	Task	For More Information
9	Complete the post-migration steps.	See, Performing Post-Migration Tasks
10	Verify the migration.	See, Verifying the Migration

14.6 Prerequisites for Migration

You must complete the following prerequisites for migrating OpenSSO Enterprise 8.0 to Access Manager 11.1.2.1.0:

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 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 10.4, "Supported Starting Points for Sun OpenSSO Enterprise Migration".

14.7 Installing Oracle Identity and Access Management 11.1.2.1.0

As part of migration process, you must freshly install Oracle Identity and Access Management 11.1.2.1.0. This 11.1.2.1.0 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 11.1.2.1.0, see "Installing Oracle Identity and Access Management (11.1.2.1.0)" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

14.8 Configuring Oracle Access Management Access Manager 11.1.2.1.0

Configure Access Manager 11.1.2.1.0, and create a domain.

For information about configuring Access Manager 11.1.2.1.0, see "Configuring Oracle Access Management" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

14.9 Generating the Assessment Report

This section describes how to generate an assessment report using the OpenSSO Agent assessment tool. The 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 11.1.2.1.0.

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.

14.9.1 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.

14.9.2 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.

14.9.3 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 14.9.1, "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
   > ```

14.9.4 Analyzing the Assessment Report

The OpenSSO Agent assessment tool generates five Comma Separated Values (CSV) files 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 11.1.2.1.0.

Table 14–3 lists the CSV files that are generated when you run the OpenSSO Agent assessment tool.

Table 14–3 Report Files Generated

File	Description
`AgentInfo.csv`	This file contains information about the J2EE and web agents that are registered with Sun OpenSSO Enterprise 8.0, and the list of agents supported in Access Manager 11.1.2.1.0.
`AuthnStoreInfo.csv`	Contains information about authentication stores.
`DashBoardInfo.csv`	Contains brief information about agents, policies, user stores, and authentication stores.
`PolicyInfo.csv`	Contains information about policies.
`UserStoreInfo.csv`	Contains information about user stores.

> **Note:** You can open the CSV files directly as CSV or using Microsoft Excel. The data in the report is displayed in the hierarchical structure with realm or subrealm name at the top followed by the data related to agents, policies, authentication stores, and user stores.

14.10 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.

14.11 Additional Steps for Incremental Migration

This section describes additional steps to be completed if you wish to perform Incremental Migration. For other modes of migration like Complete and Delta Migration, ignore this section.

When you generate the assessment report (as described in Generating the Assessment Report), a file called `IncrementalMigrationIncludeFile.txt` is generated at the location *`AssessmentToolUnzippedFolder`*`/consoleOutput/`. The content of this file is as follows:

```
REALM#TopRealm##AGENT#j2eeAgent_1##N

REALM#TopRealm##AGENT#j2eeAgent_2##N

REALM#TopRealm##POLICY#Policy1##N

REALM#TopRealm##POLICY#Policy2##N
```

Each line contains the realm name, name of the agent or policy of OpenSSO Enterprise 8.0, and the flag which is set to `N` by default. The flag value `Y` stands for 'Yes', and `N` stands for 'No'. The flag specified indicates whether an agent or policy is included or excluded in the Incremental Migration.

Note: The flag value `Y` and `N` are case-sensitive.

If you wish to include some of the agents and policies in the Incremental Migration, set the flag of the those agents and policies to `Y` in the `IncrementalMigrationIncludeFile.txt` file. Also, specify the absolute path of this file for the property `openSSOSMIncludeFilePath` in the properties file that you create in the Section 14.12, "Creating the Properties File". This includes all the agents and policies in the migration whose flags are set to `Y`.

Note: If the content of `IncrementalMigrationIncludeFile.txt` file is empty, and if you specify the absolute path of this file for the property `openSSOSMIncludeFilePath` in the properties file, no artifacts of Open Single Sign-On 8.0 will be migrated to Access Manager 11.1.2.1.0.

If you wish to exclude some of the agents and policies from the Incremental Migration, set the flag of the those agents and policies to `Y` in the `IncrementalMigrationIncludeFile.txt` file. Also, specify the absolute path of this file for the property `openSSOSMExcludeFilePath` in the properties file that you create in the Section 14.12, "Creating the Properties File". This excludes all the agents and policies from the migration whose flags are set to `Y`.

Note: If the content of `IncrementalMigrationIncludeFile.txt` file is empty, and if you specify the absolute path of this file for the property `openSSOSMExcludeFilePath` in the properties file, all the artifacts of Open Single Sign-On 8.0 will be migrated to Access Manager 11.1.2.1.0, which in turn is a complete migration.

14.12 Creating the Properties File

Create a properties file at any accessible location. For example, create a properties file by name `oam_migration.properties`.

Enter the right 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`*
- `openSSOMigrationMode=Complete/Incremental`
- `openSSOSMIncludeFilePath=`*`absolute_path_to_include_file`*
- `openSSOSMExcludeFilePath=`*`absolute_path_to_exclude_file`*

Table 14–4 describes the values you must specify for each of the properties in the properties file.

Table 14–4 Property File Values

Property	Description
`openSSOServerURL`	Specify the URL of the OpenSSO Enterprise 8.0 Administration Server. It must be specified in the format: `http://<host>:<port>/opensso` where `<host>` is the machine on which the OpenSSO Enterprise 8.0 Administration Server is running `<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 14–4 (Cont.) Property File Values

Property	Description
`openSSOServerDebugLevel`	Specify one of the following values: ■ `error` ■ `message` This value represents the debug level.
`openSSOLDAPServerURL`	Specify the URL of the LDAP server. This must be specified in the format: *`host`*`:`*`port`* where *`host`* refers to the LDAP host of the configuration store used in OpenSSO Enterprise 8.0 *`port`* refers to the LDAP port of the configuration store used in OpenSSO Enterprise 8.0 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.
`openSSOMigrationMode`	Specify the mode of migration by setting one of the following values for this property: ■ `Complete` Set this value if you wish to perform complete migration. ■ `Incremental` Set this value if you wish to perform incremental migration. Incremental Migration is dictated by the properties `openSSOSMIncludeFilePath` and `openSSOSMExcludeFilePath`. ■ `DELTA` Set this value if you wish to perform delta migration. If you do not specify any value to this property, complete migration will be performed. Also, if there is a mistake in the value `Complete` or `Incremental`, the migration mode will be considered as `Complete`, and complete migration will be performed. Note that these values are case sensitive. For more information about modes of migration, see Modes of Migration.

Table 14–4 (Cont.) Property File Values

Property	Description
openSSOSMIncludeFilePath	If you wish to perform Incremental Migration and include some of the agents and policies of OpenSSO Enterprise 8.0 in the migration, you must use the openSSOSMIncludeFilePath property. The value of the openSSOSMIncludeFilePath property must be the absolute path to the IncrementalMigrationIncludeFile.txt in which the flag of the agents and policies that you wish to include in the migration is set to Y. For more information about IncrementalMigrationIncludeFile.txt file, see "Additional Steps for Incremental Migration". If you wish to perform incremental migration with the openSSOSMIncludeFilePath property, comment out the openSSOSMExcludeFilePath property. If you specify both openSSOSMIncludeFilePath and openSSOSMExcludeFilePathproperties when you perform incremental migration, the openSSOSMIncludeFilePath property takes precedence over openSSOSMExcludeFilePath property, and the openSSOSMExcludeFilePath property is ignored. For complete migration, ignore this property.
openSSOSMExcludeFilePath	If you wish to perform Incremental Migration and exclude some of the agents and policies of OpenSSO Enterprise 8.0 from migration, you must use the openSSOSMExcludeFilePath property. The value of the openSSOSMExcludeFilePath property must be the absolute path to the IncrementalMigrationIncludeFile.txt in which the flag of the agents and policies that you wish to exclude from the migration is set to Y. For more information about IncrementalMigrationIncludeFile.txt file, see Additional Steps for Incremental Migration. If you wish to perform incremental migration with the openSSOSMExcludeFilePath property, comment out the openSSOSMIncludeFilePath property. If you specify both openSSOSMExcludeFilePath and openSSOSMIncludeFilePath properties when you perform incremental migration, the openSSOSMIncludeFilePath property takes precedence over openSSOSMExcludeFilePath property, and the openSSOSMExcludeFilePath property is ignored. For complete migration, ignore this property.

Note: Do not specify any value for openSSOAdminPassword and openSSOLDAPBindPwd properties.

If the file path specified for openSSOSMExcludeFilePath or openSSOSMExcludeFilePath is incorrect, or if the provided file path is not readable due to permission issues, appropriate error message will be displayed. You can also view this in the log file.

If you perform Incremental Migration and IncrementalMigrationIncludeFile.txt file is empty, the mode changes to Complete, and Complete Migration is performed.

14.13 Migrating the Artifacts of OpenSSO Enterprise 8.0 to Access Manager 11.1.2.1.0

Before you start the actual migration of the artifacts from OpenSSO Enterprise 8.0 to Access Manager 11.1.2.1.0, make sure that you have generated the assessment report (as described in Section 14.9, "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 11.1.2.1.0, do the following:

1. If you wish to perform Incremental Migration, make sure you have completed the additional steps as described in Section 14.11, "Additional Steps for Incremental Migration".
2. Make sure you have created the properties file as described in Section 14.12, "Creating the Properties File".
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. 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.

5. Run the following command to migrate the artifacts of OpenSSO Enterprise 8.0 to Access Manager 11.1.2.1.0:

   ```
   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 14.2, "Modes of Migration".

When the migration is complete, the WLST console displays a message stating the result of the migration.

14.14 Performing Post-Migration Tasks

After you migrate OpenSSO Enterprise 8.0 to Access Manager 11.1.2.1.0, 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 11.1.2.1.0. 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 11.1.2.1.0 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 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 11.1.2.1.0 console. To do this, complete the following steps:

   a. Log in to the Oracle Access Management 11.1.2.1.0 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**.

14.15 Verifying the Migration

To verify the migration, do the following:

1. Log in to the Oracle Access Management 11.1.2.1.0 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 11.1.2.1.0 console.
- *port* refers to the designated bind port for the Oracle Access Management 11.1.2.1.0 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 11.1.2.1.0.

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.

15

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 (11.1.2.1.0).

The chapter contains the following sections:

15.1 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 11.1.2.1.0.

OpenSSO Agent Assessment Tool

The OpenSSO Agent assessment tool reads the agents and policies from the Sun Java System Access Manager 7.1 server, analyzes the agents and the policy elements which can be migrated to Access Manager 11.1.2.1.0, and generates an assessment report. The generated report provides the 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 11.1.2.1.0 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 11.1.2.1.0 and what cannot be migrated to Access Manager 11.1.2.1.0 based on the understanding of the supported artifacts in Access Manager 11.1.2.1.0.

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 11.1.2.1.0:

- 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".

15.2 Modes of Migration

This section describes the three modes of migration that you can perform using the procedure described in this chapter. The following are the two modes of migration:

- Complete Migration
- Incremental Migration
- Delta Migration

15.2.1 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 11.1.2.1.0. 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 11.1.2.1.0 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.

15.2.2 Incremental Migration

Incremental Migration is referred to as Selective Migration, as you can select the agents and polices of Sun Java System Access Manager 7.1 that you wish to migrate to Access Manager 11.1.2.1.0. You can perform this migration multiple times with different sets of agents and policies, and therefore it is called Incremental Migration. Selecting only the user stores or authentication stores for incremental migration is not supported. When you select the agents and policies for incremental migration, you must also select the respective user stores and authentication stores.

> **Note:** You can perform Incremental Migration after performing Complete Migration, which will be referred to as Incremental Delta.
>
> You can perform a Complete Migration after multiple Incremental Migration. In this case, the Complete Migration ignores the agents and policies that are already migration as part of the previous Incremental Migrations.
>
> When you perform multiple Incremental Migrations by selecting the artifacts (agents and policies) that are already migrated, those artifacts are ignored, and the Incremental Migration migrates only the non-migrated artifacts.

15.2.3 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 11.1.2.1.0. 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 11.1.2.1.0 configuration store is retrieved, is incremented by one, and is saved back to Access Manager 11.1.2.1.0 configuration store.

The procedure to perform 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 Sun Java System Access Manager 7.1 that are compatible with Access Manager 11.1.2.1.0. 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 Sun Java System Access Manager 7.1 to Access Manager 11.1.2.1.0.

- 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.
- 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 11.1.2.1.0 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 Sun Java System Access Manager 7.1 to Access Manager 11.1.2.1.0.

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 11.1.2.1.0:

- **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 11.1.2.1.0. All the auto policies can be migrated to Access Manager 11.1.2.1.0.
- **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 11.1.2.1.0. Semi policies are not migrated to Access Manager 11.1.2.1.0.
- **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 11.1.2.1.0. Manual policies are not migrated to Access Manager 11.1.2.1.0.

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 11.1.2.1.0) are not supported in Access Manager 11.1.2.1.0.

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 11.1.2.1.0.

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 11.1.2.1.0.
  - The attribute Terminate session of this condition is ignored during migration as the appropriate mapping of this attribute does not exist in Access Manager 11.1.2.1.0.
- Authentication by Module Instance
  - This condition of Sun Java System Access Manager 7.1 policy is migrated to Access Manager 11.1.2.1.0 as AuthN scheme, and not as a condition.
  - Table 15–1 lists the authentication modules of Sun Java System Access Manager 7.1 that are migrated and mapped with the AuthN scheme into Access Manager 11.1.2.1.0.

Table 15–1 Mapping of Authentication Module

Authentication Module in Sun Java System Access Manager 7.1	Authentication Plug-in in Access Manager 11.1.2.1.0
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 11.1.2.1.0 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 11.1.2.1.0.

    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 11.1.2.1.0 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 11.1.2.1.0 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 11.1.2.1.0.
  - 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 11.1.2.1.0.
  - 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 11.1.2.1.0.
  - The condition `DNS name` is not supported in Access Manager 11.1.2.1.0.
- LDAP Filter Condition
  - This condition in Sun Java System Access Manager 7.1 policy is mapped to `Identity condition` in Access Manager 11.1.2.1.0.
  - 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 11.1.2.1.0.
- 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 11.1.2.1.0.
  - 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 11.1.2.1.0 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 11.1.2.1.0. 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 11.1.2.1.0 with the type Http header.

15.3.3 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 11.1.2.1.0.

OpenSSO Enterprise has three types of user stores:

- **Active Directory**: This user store can be migrated to Access Manager 11.1.2.1.0.
- **Generic LDAPv3**: This user store can be migrated to Access Manager 11.1.2.1.0.
- **Sun DS with OpenSSO schema**: This user store cannot be migrated to Access Manager 11.1.2.1.0, as no supported data store type is available in 11.1.2.1.0.

15.3.4 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 11.1.2.1.0.

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 11.1.2.1.0:

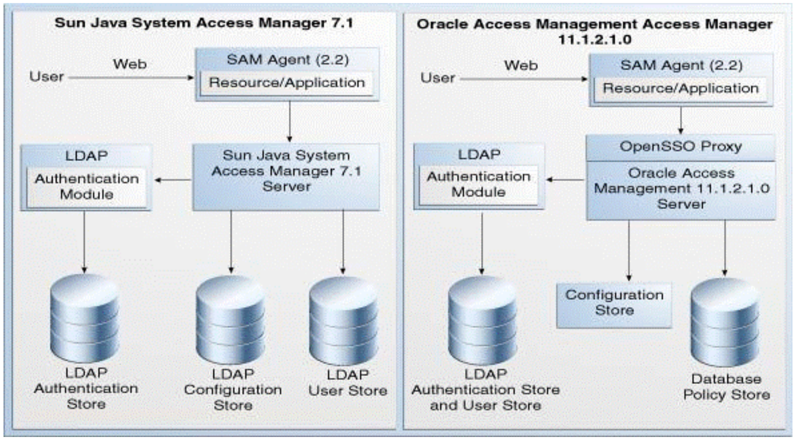
- LDAP in Sun Java System Access Manager 7.1 is mapped to OAM LDAP in Access Manager 11.1.2.1.0.
- Certificate in Sun Java System Access Manager 7.1 is mapped to X509 in Access Manager 11.1.2.1.0.
- Windows Desktop SSO in Sun Java System Access Manager 7.1 is mapped to Kerberos Access Manager 11.1.2.1.0.

All authentication stores with type LDAP are migrated to Access Manager 11.1.2.1.0 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 Java System Access Manager 7.1 and Access Manager 11.1.2.1.0.

Figure 15–1 Sun Java System Access Manager 7.1 and Access Manager 11.1.2.1.0 Topologies


Sun Java System Access Manager 7.1
User
Web
SAM Agent (2.2)
Resource/Application
LDAP
Authentication Module
Sun Java System Access Manager 7.1 Server
LDAP Authentication Store
LDAP Configuration Store
LDAP User Store
Oracle Access Management Access Manager 11.1.2.1.0
User
Web
SAM Agent (2.2)
Resource/Application
LDAP
Authentication Module
OpenSSO Proxy
Oracle Access Management 11.1.2.1.0 Server
Configuration Store
LDAP Authentication Store and User Store
Database Policy Store

15.5 Migration Roadmap

Table 15–2 lists the steps to migrate Sun Java System Access Manager 7.1 to Access Manager 11.1.2.1.0.

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 11.1.2.1.0.	See, Installing Oracle Identity and Access Management 11.1.2.1.0
3	Configure Oracle Access Management Access Manager 11.1.2.1.0.	See, Configuring Oracle Access Manager 11.1.2.1.0
4	Generate the assessment report, and analyze what artifacts can be migrated to Access Manager 11.1.2.1.0. You can perform this task multiple times.	See, Generating the Assessment Report
5	Start the WebLogic Administration Server.	See, Starting the WebLogic Administration Server
6	If you wish to perform Incremental Migration, complete the additional steps.	See, Additional Steps for Incremental Migration
7	Create the properties file.	See, Creating the Properties File
8	Migrate Sun Java System Access Manager 7.1 to Access Manager 11.1.2.1.0 by running the migration tool.	See, Migrating the Artifacts of Sun Java System Access Manager 7.1 to OAM 11.1.2.1.0
9	Complete the post-migration steps.	See, Performing Post-Migration Tasks
10	Verify the migration.	See, Verifying the Migration

15.6 Prerequisites for Migration

You must complete the following prerequisites for migrating Sun Java System Access Manager 7.1 to Access Manager 11.1.2.1.0:

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 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 10.5, "Supported Starting Points for Sun Java System Access Manager Migration".

15.7 Installing Oracle Identity and Access Management 11.1.2.1.0

As part of the migration process, you must freshly install Oracle Identity and Access Management 11.1.2.1.0 This 11.1.2.1.0 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 11.1.2.1.0, see "Installing Oracle Identity and Access Management (11.1.2.1.0)" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

15.8 Configuring Oracle Access Manager 11.1.2.1.0

After you install Oracle Identity and Access Management 11.1.2.1.0, you must configure Access Manager 11.1.2.1.0 in a domain.

For more information about configuring Access Manager 11.1.2.1.0, 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. The 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 11.1.2.1.0.

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.

15.9.1 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.

15.9.2 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.

15.9.3 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**.

15.9.4 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 15.9.1, "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
> ```

15.9.5 Analyzing the Assessment Report

The assessment tool generates five Comma Separated Values (CSV) 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 11.1.2.1.0.

Table 15–3 lists the CSV files that are generated when you run the assessment tool.

Table 15–3 Report Files Generated

File	Description
`AgentInfo.csv`	This file contains information about the J2EE and web agents that are registered with Sun Java System Access Manager 7.1, and the list of agents supported in Access Manager 11.1.2.1.0.
`AuthnStoreInfo.csv`	This file contains information about authentication stores.
`DashBoardInfo.csv`	Contains brief information about agents, policies, user stores, and authentication stores.
`PolicyInfo.csv`	Contains information about policies.
`UserStoreInfo.csv`	Contains information about user stores.

> **Note:** You can open the CSV files directly as CSV or using Microsoft Excel. The data in the report is displayed in the hierarchical structure with realm or subrealm name at the top followed by the data related to agents, policies, authentication stores, and 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 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.

15.11 Additional Steps for Incremental Migration

This section describes additional steps to be completed if you wish to perform Incremental Migration. For other modes of migration like Complete and Delta Migration, ignore this section.

When you generate the assessment report (as described in Generating the Assessment Report), a file called `IncrementalMigrationIncludeFile.txt` is generated at the location *AssessmentToolUnzippedFolder*/consoleOutput/. The content of this file is as follows:

```
REALM#TopRealm##AGENT#j2eeAgent_1##N

REALM#TopRealm##AGENT#j2eeAgent_2##N

REALM#TopRealm##POLICY#Policy1##N

REALM#TopRealm##POLICY#Policy2##N
```

Each line contains the realm name, name of the agent or policy of Sun Java System Access Manager 7.1, and the flag which is set to `N` by default. The flag value `Y` stands for 'Yes', and `N` stands for 'No'. The flag specified indicates whether an agent or policy is included or excluded in the Incremental Migration.

Note: The flag value `Y` and `N` are case-sensitive.

If you wish to include some of the agents and policies in the Incremental Migration, set the flag of the those agents and policies to `Y` in the `IncrementalMigrationIncludeFile.txt` file. Also, specify the absolute path of this file for the property `openSSOSMIncludeFilePath` in the properties file that you create in the Section 15.12, "Creating the Properties File". This includes all the agents and policies in the migration whose flags are set to `Y`.

Note: If the content of `IncrementalMigrationIncludeFile.txt` file is empty, and if you specify the absolute path of this file for the property `openSSOSMIncludeFilePath` in the properties file, no artifacts of Sun Java System Access Manager 7.1 will be migrated to Access Manager 11.1.2.1.0.

If you wish to exclude some of the agents and policies from the Incremental Migration, set the flag of the those agents and policies to `Y` in the `IncrementalMigrationIncludeFile.txt` file. Also, specify the absolute path of this file for the property `openSSOSMExcludeFilePath` in the properties file that you create in the Section 15.12, "Creating the Properties File". This excludes all the agents and policies from the migration whose flags are set to `Y`.

Note: If the content of `IncrementalMigrationIncludeFile.txt` file is empty, and if you specify the absolute path of this file for the property `openSSOSMExcludeFilePath` in the properties file, all the artifacts of Sun Java System Access Manager 7.1 will be migrated to Access Manager 11.1.2.1.0, which in turn is a complete migration.

15.12 Creating the Properties File

Create a properties file at any accessible location. For example, create a properties file by name `oam_migration.properties`.

Enter the right 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`*
- `openSSOMigrationMode=Complete/Incremental`
- `openSSOSMIncludeFilePath=`*`absolute_path_to_include_file`*
- `openSSOSMExcludeFilePath=`*`absolute_path_to_exclude_file`*

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 Sun Java System Access Manager 7.1 Server. It must be specified in the format: `http://<host>:<port>/amserver` where `<host>` is the machine on which the Sun Java System Access Manager 7.1 Administration Server is running `<port>` is the port number of the Sun Java System Access Manager Administration Server
`openSSOAdminUser`	Specify the username of the Sun Java System Access Manager Administration Server.
`openSSOAdminPassword`	Do not specify any value for this property. The migration tool prompts you for the Sun Java System Access Manager admin password when you run the migration command, as described in step-4.
`openSSOServerDebugLevel`	Specify one of the following values: ■ `error` ■ `message` This value represents the debug level.
`openSSOLDAPServerURL`	Specify the URL of the LDAP server. This must be specified in the format: *`host`*`:`*`port`* where *`host`* refers to the LDAP host of the configuration store used in Sun Java System Access Manager 7.1 *`port`* refers to the LDAP port of the configuration store used in Sun Java System Access Manager 7.1 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 Sun Java System Access Manager.
`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.

Table 15–4 (Cont.) Property File Values

Property	Description
openSSOMigrationMode	Specify the mode of migration by setting one of the following values for this property: ■ Complete Set this value if you wish to perform Complete Migration. ■ Incremental Set this value if you wish to perform Incremental Migration. Incremental Migration is dictated by the properties openSSOSMIncludeFilePath and openSSOSMExcludeFilePath. ■ Delta Set this value if you wish to perform delta migration. If you do not specify any value to this property, Complete Migration will be performed. Also, if there is a mistake in the value Complete or Incremental, the migration mode will be considered as Complete, and complete migration will be performed. Note that these values are case sensitive. For more information about modes of migration, see Modes of Migration.
openSSOSMIncludeFilePath	If you wish to perform Incremental Migration and include some of the agents and policies of Sun Java System Access Manager 7.1 in the migration, you must use the openSSOSMIncludeFilePath property. The value of the openSSOSMIncludeFilePath property must be the absolute path to the IncrementalMigrationIncludeFile.txt in which the flag of the agents and policies that you wish to include in the migration is set to Y. For more information about IncrementalMigrationIncludeFile.txt file, see "Additional Steps for Incremental Migration". If you wish to perform Incremental Migration with the openSSOSMIncludeFilePath property, comment out the openSSOSMExcludeFilePath property. If you specify both openSSOSMIncludeFilePath and openSSOSMExcludeFilePath properties when you perform incremental migration, the openSSOSMIncludeFilePath property takes precedence over openSSOSMExcludeFilePath property, and the openSSOSMExcludeFilePath property is ignored. For complete migration, ignore this property.

Table 15–4 (Cont.) Property File Values

Property	Description
`openSSOSMExcludeFilePath`	If you wish to perform Incremental Migration and exclude some of the agents and policies of Sun Java System Access Manager 7.1 from migration, you must use the `openSSOSMExcludeFilePath` property. The value of the `openSSOSMExcludeFilePath` property must be the absolute path to the `IncrementalMigrationIncludeFile.txt` in which the flag of the agents and policies that you wish to exclude from the migration is set to `Y`. For more information about `IncrementalMigrationIncludeFile.txt` file, see Additional Steps for Incremental Migration. If you wish to perform incremental migration with the `openSSOSMExcludeFilePath` property, comment out the `openSSOSMIncludeFilePath` property. If you specify both `openSSOSMExcludeFilePath` and `openSSOSMIncludeFilePath`properties when you perform incremental migration, the `openSSOSMIncludeFilePath` property takes precedence over `openSSOSMExcludeFilePath` property, and the `openSSOSMExcludeFilePath` property is ignored. For complete migration, ignore this property.

Note: Do not specify any value for `openSSOAdminPassword` and `openSSOLDAPBindPwd` properties.

If the file path specified for `openSSOSMExcludeFilePath` or `openSSOSMExcludeFilePath` is incorrect, or if the provided file path is not readable due to permission issues, appropriate error message will be displayed. You can also view this in the log file.

If you perform Incremental Migration and `IncrementalMigrationIncludeFile.txt` file is empty, the mode changes to Complete, and Complete Migration is performed.

15.13 Migrating the Artifacts of Sun Java System Access Manager 7.1 to OAM 11.1.2.1.0

Before you start the actual migration of the artifacts from Sun Java System Access Manager 7.1 to Access Manager 11.1.2.1.0, 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 11.1.2.1.0.

To migrate Sun Java System Access Manager 7.1 to Access Manager 11.1.2.1.0, do the following:

1. If you wish to perform Incremental Migration, make sure you have completed the additional steps as described in Section 15.11, "Additional Steps for Incremental Migration".

2. Make sure you have created the properties file as described in Section 15.12, "Creating the Properties File".

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. 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

5. Run the following command to migrate the artifacts of Sun Java System Access Manager 7.1 to Access Manager 11.1.2.1.0:

```
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 15.2, "Modes of Migration".

When the migration is complete, the WLST console displays a message stating the result of the migration.

15.14 Performing Post-Migration Tasks

After you migrate Sun Java System Access Manager 7.1 to Access Manager 11.1.2.1.0, 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 11.1.2.1.0 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 11.1.2.1.0. 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 11.1.2.1.0 console using the following URL:

   ```
   http://host:port/oamconsole
   ```

where *host* is the machine on which Access Manager 11.1.2.1.0 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 11.1.2.1.0 console. To do this, complete the following steps:

   a. Log in to the Oracle Access Management 11.1.2.1.0 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**.

15.15 Verifying the Migration

To verify the migration, do the following:

1. Log in to the Oracle Access Management 11.1.2.1.0 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 11.1.2.1.0 console.
   - *port* refers to the designated bind port for the Oracle Access Management 11.1.2.1.0 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 11.1.2.1.0.

2. Access any protected page using the URL. The URL now redirects you to the Oracle Access Management 11.1.2.1.0 Server login page. Upon successful authentication, it should perform a successful authorization and you should be able to access the resource successfully.

16

Coexistence of Oracle Access Manager 10*g* with Oracle Access Management Access Manager 11.1.2.1.0

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 (11.1.2.1.0) deployments coexist, after you migrate from Oracle Access Manager 10*g* to Oracle Access Management Access Manager 11.1.2.1.0. In this coexistence scenario, the Oracle Access Manager 10*g* Server does the authentication for all the resources.

This chapter contains the following sections:

16.1 Coexistence Overview

During the process of migration from Oracle Access Manager 10*g* to Access Manager 11.1.2.1.0, you can have both Oracle Access Manager 10*g* and Access Manager 11.1.2.1.0 deployments coexisting, so that some applications are protected by Oracle Access Manager 10*g* while others are protected by Access Manager 11.1.2.1.0. 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.

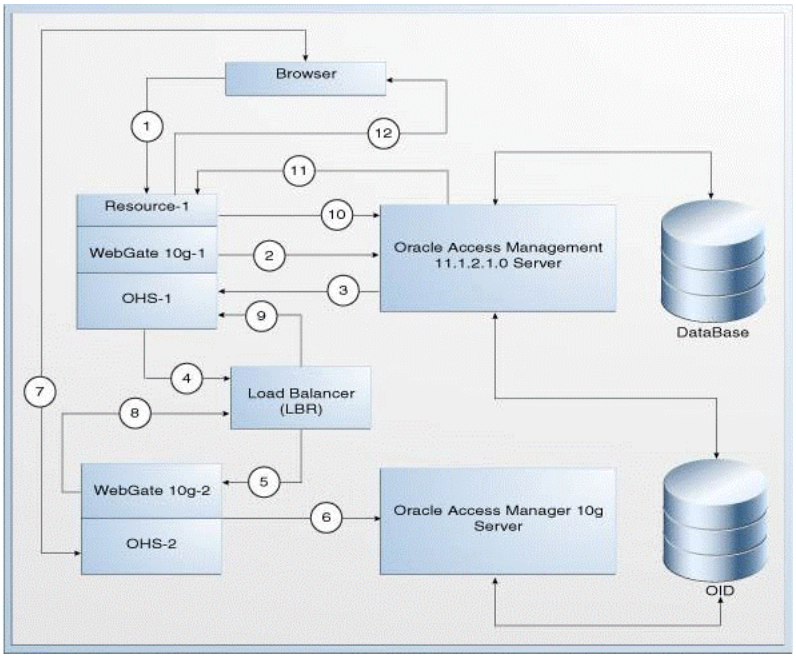
In this mode, Access Manager 11.1.2.1.0 protects the migrated applications and any new applications registered with Access Manager 11.1.2.1.0; whereas Oracle Access Manager 10*g* continues to protect the applications that are not migrated to Access Manager 11.1.2.1.0.

In this coexistence mode, Oracle Access Manager 10*g* performs the authentication for all the resources protected by Access Manager 11.1.2.1.0.

16.2 Coexistence Topology

Figure 16–1 illustrates how the Oracle Access Manager 10*g* Server coexists with the Access Manager 11.1.2.1.0 Server.

Figure 16–1 Coexistence of Oracle Access Manager 10g with Access Manager 11.1.2.1.0



The topology consists of disjoint Oracle Access Manager 10*g* and Access Manager 11.1.2.1.0 setups. The numbers 1-12 in the topology show the sequence in which the requests flow in the coexistence environment. Table 16–1 describes the request flow.

This coexistence setup contains the following:

- Oracle Access Manager 10*g* WebGate partners registered against Access Manager 11.1.2.1.0 Server.
- Oracle Access Manager 10*g* WebGate partners registered against Oracle Access Manager 10*g* Server.

Topology Description

- WebGate 10*g*-1: This refers to the 10*g* or 11*g* WebGate partner registered with Access Manager 11.1.2.1.0 Server. It is deployed on Oracle HTTP Server 11*g* named OHS-1. WebGate 10*g*-1 protects the resources or applications that are migrated to Access Manager 11.1.2.1.0.
- WebGate 10*g*-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 11.1.2.1.0, 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 11.1.2.1.0 Managed Server's host and port. It front-ends the credential collector of Access Manager 11.1.2.1.0. For this reason, you must use the OHS module for WebLogic.
- Resource-1: This is any resource protected by Access Manager 11.1.2.1.0 Server.
- Load Balancer (LBR): This is a logical load balancer that maps to the configuration in Access Manager 11.1.2.1.0.

Table 16–1 describes the request flow. The numbers in the **Step** column correspond to the numbers shown in the topology in Figure 16–1.

Table 16–1 Request Flow

Step	Description
1	User requests access to Resource-1, which is protected by Access Manager 11.1.2.1.0 Server at the following URL: http://OHS-1:port/Resource1 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 11.1.2.1.0 server to obtain the Access Manager 11.1.2.1.0 Server authentication end point.
4 and 5	WebGate 10*g*-1 redirects to the authentication end point of Access Manager 11.1.2.1.0 Server. This goes to the OHS-2 (WebGate 10*g*-2), as OHS-2 acts as reverse proxy for the Access Manager 11.1.2.1.0 server's credential collector.
6	WebGate 10*g*-2 is registered against the Oracle Access Manager 10*g* Server, and Access Manager 11.1.2.1.0 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 11.1.2.1.0 Server authentication end point, the request to Access Manager 11.1.2.1.0 Server authentication end point passes to the Access Manager 11.1.2.1.0 Managed Server port.

Table 16–1 (Cont.) Request Flow

Step	Description
11	The Access Manager 11.1.2.1.0 server asserts (using header **OAM_REMOTE_USER**) as `Resource-1` is protected at Access Manager 11.1.2.1.0 server using the **OAM10gScheme**. All relevant headers and cookies are set and redirected to Resource-1.

16.3 Task Roadmap

Table 16–2 lists the steps to set up and configure the topology shown in Figure 16–1.

Table 16–2 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. 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 11.1.2.1.0 Managed Server.	See, Configuring OHS-2 as a Reverse Proxy for Access Manager 11.1.2.1.0 Managed Server
5	Update the authentication module **LDAPNoPasswordAuthModule** in Access Manager 11.1.2.1.0, and point the User Identity Store to the data source that is created in Access Manager 11.1.2.1.0 as a result of migration.	See, Updating LDAPNoPasswordAuthModule in Access Manager 11.1.2.1.0

Table 16–2 (Cont.) Tasks to be Completed

Ta sk No	Task	For More Information
6	Install two WebGates: `WebGate 10g-1` and `WebGate 10g-2`. `WebGate 10g-1` should be deployed on `OHS-1`, and configured with Access Manager 11.1.2.1.0 Server. This WebGate can be a 10*g* or and 11*g* WebGate. `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. 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 primary cookie domains for the WebGates.	See, Configuring Primary Cookie Domains for WebGates
8	Protect all the resources at Access Manager 11.1.2.1.0.	See, Protecting Resources at Access Manager 11.1.2.1.0
9	Protect the Access Manager 11.1.2.1.0 authentication end point URL in Oracle Access Manager 10*g*.	See, Protecting the Authentication End Point URL of Access Manager 11.1.2.1.0 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 11.1.2.1.0 server.	See, Configuring Logout Settings
11	Configure the session management.	See, Configuring Session Management Settings
12	Verify the configuration.	See, Verifying the Configuration

16.4 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 11.1.2.1.0.

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 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 11.1.2.1.0, see Section 10.6, "Supported Starting Points for Coexistence of Oracle Access Manager 10g With Oracle Access Management Access Manager 11.1.2.1.0".
3. Migrate the artifacts of Oracle Access Manager 10*g* to Access Manager 11.1.2.1.0. For more information, see Chapter 11, "Migrating Oracle Access Manager 10g Environments".
4. Make sure that Oracle Access Manager 10*g* and Access Manager 11.1.2.1.0 share the same user store.
5. Make sure that the Oracle Access Manager 10*g* and the Oracle Access Management 11.1.2.1.0 servers are up and running.

16.5 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 16–1). Alternatively, you can use the Oracle HTTP Server instances that exist after migration from Oracle Access Manager 10*g* to Access Manager 11.1.2.1.0.

For more information, see "Installing and Configuring Oracle HTTP Server 11*g*" in the *Oracle Fusion Middleware Installing WebGates for Oracle Access Manager*.

16.6 Configuring OHS-2 as a Reverse Proxy for Access Manager 11.1.2.1.0 Managed Server

You must configure `OHS-2` as a reverse proxy for Access Manager 11.1.2.1.0 server, so that it front ends the Access Manager 11.1.2.1.0 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 11.1.2.1.0 server, do the following:

1. Set up `OHS-2` to forward requests with the URL prefix "`/oam`" to the Access Manager 11.1.2.1.0 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 11.1.2.1.0 Server.
2. Restart `OHS-2`.
3. Log in to the Oracle Access Management 11.1.2.1.0 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 11.1.2.1.0 console (Administration Server)

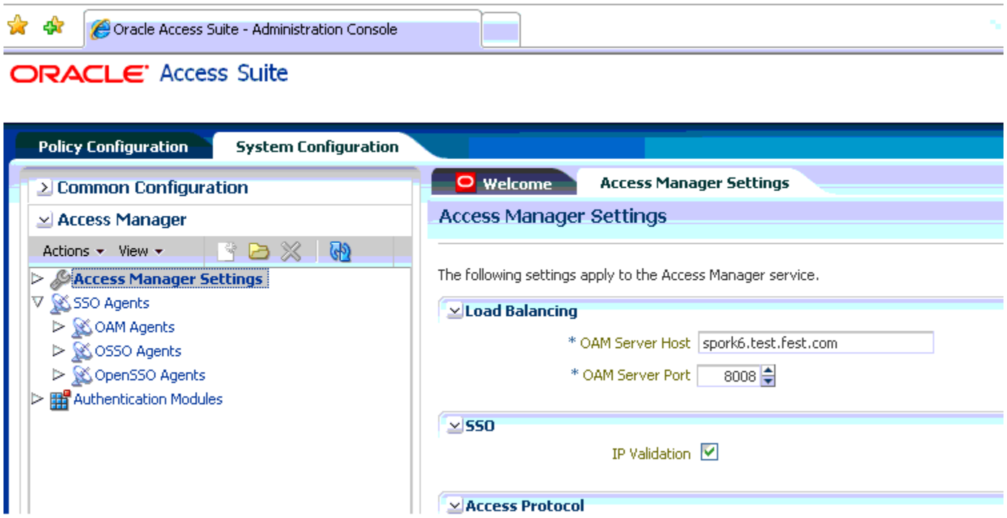
port refers to the designated bind port for the Oracle Access Management 11.1.2.1.0 console, which is the same as the bind port for the Administration Server

`/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 16–2 shows the Access Manager 11.1.2.1.0 console where you must change the Access Manager Settings.

Figure 16–2 Changing the Load Balancing Settings



Access Manager Settings

The following settings apply to the Access Manager service.

Load Balancing

* OAM Server Host sporkó.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 11.1.2.1.0 Server, you must make changes to the Access Manager 11.1.2.1.0 Server, so that the Access Manager 11.1.2.1.0 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.

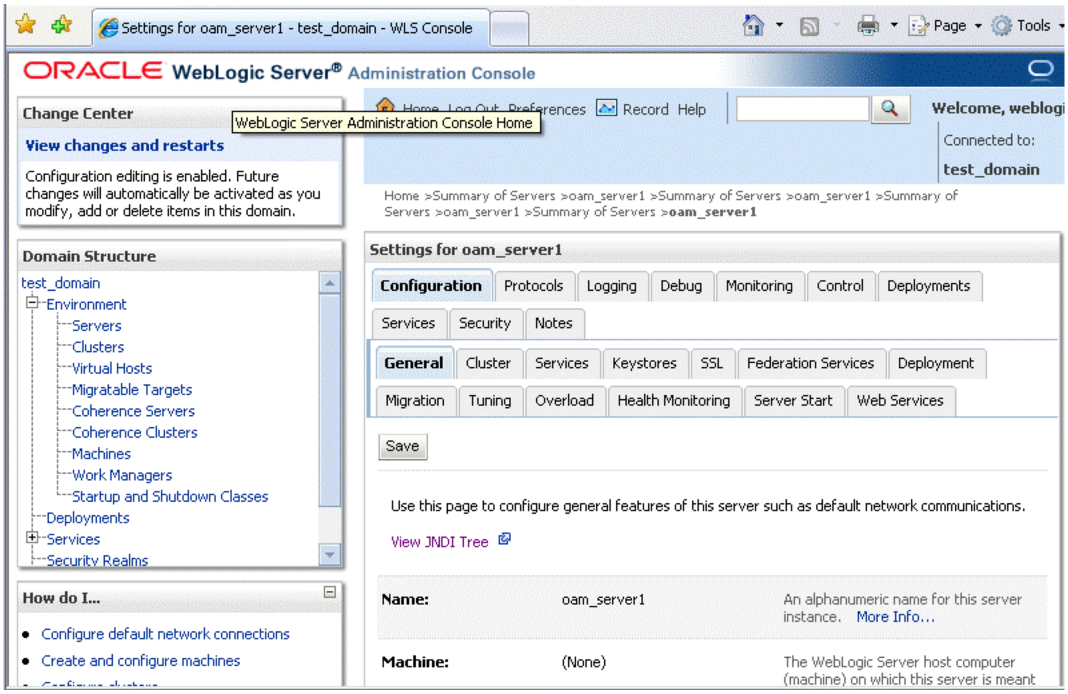
   c. Select **Servers**.

   d. Select **OAM Server** from **Summary of Servers** in the right panel.

e. Select the **Configuration** tab, and then click the **General** tab.

Figure 16–3 shows the tabs that you must select in WebLogic console.

Figure 16–3 Selecting the OAM Server



Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

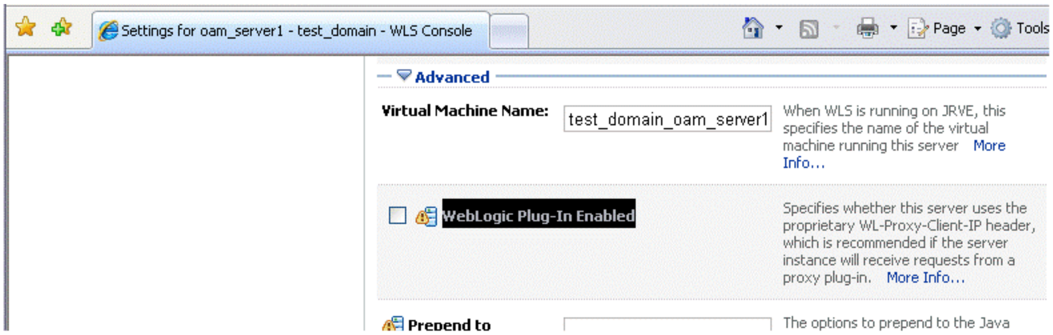
Use this page to configure general features of this server such as default network communications.

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 16–4 shows the checkbox that you must select.

Figure 16–4 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 Server, and the Access Manager 11.1.2.1.0 Managed Server.

16.7 Updating LDAPNoPasswordAuthModule in Access Manager 11.1.2.1.0

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 11.1.2.1.0 as a result of migration. To do this, complete the following steps:

1. Log in to the Oracle Access Management 11.1.2.1.0 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 11.1.2.1.0 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 11.1.2.1.0 as a result of migration.

16.8 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 11.1.2.1.0 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 11.1.2.1.0 WebGate. You must install a 10*g* or 11*g* WebGate on Oracle HTTP Server 11*g* (`OHS-1`), as shown in Figure 16–1, and configure it with the Access Manager 11.1.2.1.0 Server.

  For information on installing 10*g* WebGate, and configuring it with the Access Manager 11.1.2.1.0 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 11.1.2.1.0 server, see "Installing and Configuring Oracle HTTP Server 11*g* Webgate for OAM" in the *Oracle Fusion Middleware Installing WebGates for Oracle Access Manager*.

- `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 16–1, 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 11.1.2.1.0, see "Managing 10*g* Webgates with Oracle Access Manager 11*g*" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.

16.9 Configuring Primary Cookie Domains for WebGates

If the resource WebGate (`WebGate 10g-1`) configured with the Access Manager 11.1.2.1.0 Server is of type 10*g* WebGate, you must set separate primary cookie domains for each of the WebGate instances (`WebGate 10g-1` and `WebGate 10g-2`).

There are two ways of achieving this. These two approaches depend on the number of WebGates whose cookie domains need to be separated. You must follow one of the following ways:

- Separating Cookie Domain of All the WebGates
- Separating Cookie Domain of the Authentication WebGate

16.9.1 Separating Cookie Domain of All the WebGates

You must follow this approach if the total number of WebGates whose primary cookie domain needs to be changed is less. In this approach, the primary cookie domain of all the WebGates configured with Oracle Access Manager 10*g* server (for example, `WebGate 10g-2`) must be different from the primary cookie domain of all the WebGates configured with Access Manager 11.1.2.1.0 server (for example, `WebGate 10g-1`). To achieve this, you can either change the primary cookie domain of the old 10*g* WebGate, or the newly migrated 10*g* WebGate.

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 11.1.2.1.0 server, do the following:

   a. Log in to the Oracle Access Management 11.1.2.1.0 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 "Create Virtual Hosts to Support Identity Management" 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).

16.9.2 Separating Cookie Domain of the Authentication WebGate

If the number of WebGates in 10*g* deployment and the newly migrated deployment is more, the approach of configuring separate primary cookie domains for the WebGates (as described in Section 16.9.1, "Separating Cookie Domain of All the WebGates") is not feasible. Therefore, you must follow this approach.

In this approach, you must separate the primary cookie domain of the authentication WebGate (`WebGate 10g-2`):

1. Separating the Primary Cookie Domain of WebGate 10g-2
2. Changing the Authentication Scheme in 10g Deployment

16.9.2.1 Separating the Primary Cookie Domain of WebGate 10*g*-2

You must configure a separate primary cookie domain for the authentication WebGate (`WebGate 10g-2`). All the other WebGates will have the same primary cookie domain. That is, the primary cookie domain for the WebGates configured with Access Manager 11*g* Server (like `WebGate 10g-1` and others, if any) and the WebGates configured with Oracle Access Manager 10*g* (other than `WebGate 10g-2`) is same.

In such deployment, if the user interchanges the resource request between the WebGates of 10g deployment and the migrated deployment, or vice versa, the `ObSSOcookies` is overwritten by both the WebGates, and the end user does not see any difference in the behavior.

To configure separate primary cookie domain for the authentication WebGate (`WebGate 10g-2`), 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).

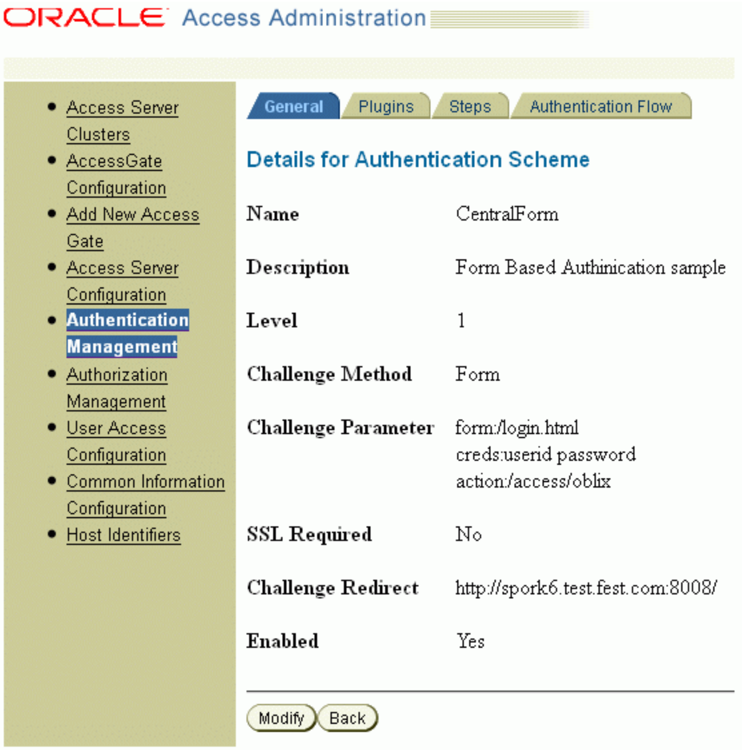
16.9.2.2 Changing the Authentication Scheme in 10*g* Deployment

You must configure centralized authentication point for the resources of 10*g* that coexists with the 11*g* deployment. To do this, you must modify all the existing authentication schemes which protect the 10*g* resources, by setting the URL of the authentication WebGate (`WebGate 10g-2`) as the value for the parameter **Challenge Redirect** in all the authentication schemes.

For more information about modifying the 10*g* authentication scheme, see "Modifying an Authentication Scheme" in the *Oracle Access Manager Access Administration Guide* for release 10g (10.1.4.3).

Figure 16–5 shows the sample authentication scheme in which the URL of the authentication WebGate specified as the value for the parameter **Challenge Redirect**.

Figure 16–5 Sample Authentication Scheme



Details for Authentication Scheme

Name	CentralForm
Description	Form Based Authinication sample
Level	1
Challenge Method	Form
Challenge Parameter	form:/login.html creds:userid password action:/access/oblix
SSL Required	No
Challenge Redirect	http://spork6.test.fest.com:8008/
Enabled	Yes

16.10 Protecting Resources at Access Manager 11.1.2.1.0

Resource `WebGate 10g-1`, which is configured with the Access Manager 11.1.2.1.0 Server has to protect the resources with the special authentication scheme (**OAM10gScheme**).

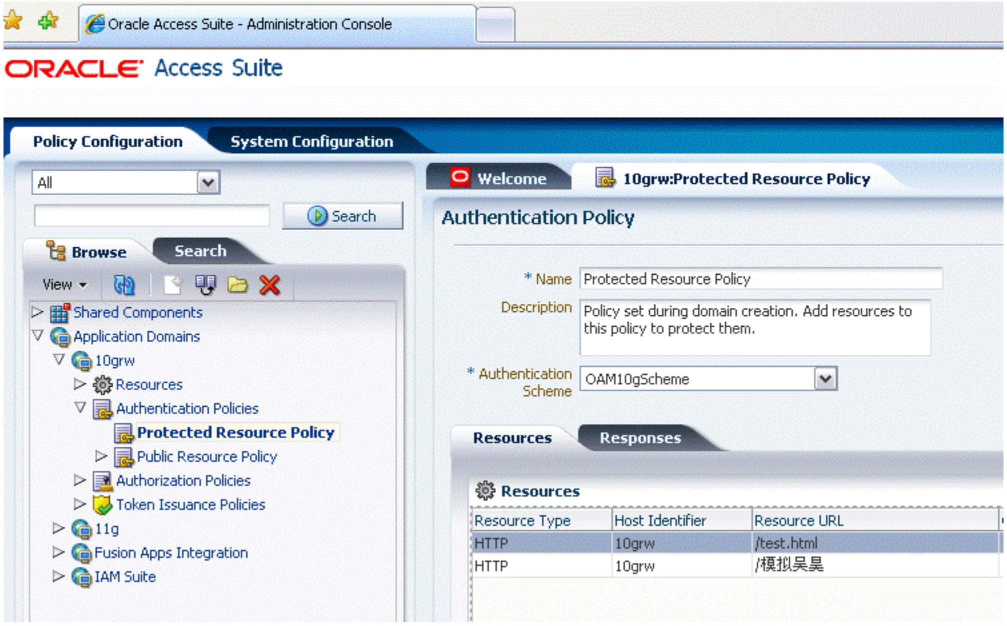
To achieve this, you must either change the authentication scheme of the existing authentication policy, or you must have a new application domain and create a new policy.

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 16–6 shows the authentication scheme that you must select for the authentication policy which protects the resources.

Figure 16–6 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

16.11 Protecting the Authentication End Point URL of Access Manager 11.1.2.1.0 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 11.1.2.1.0 by protecting the authentication end point URL of Access Manager 11.1.2.1.0.

The following resource must be protected by an Oracle Access Manager 10*g* policy:

/oam/server/obrareq.cgi

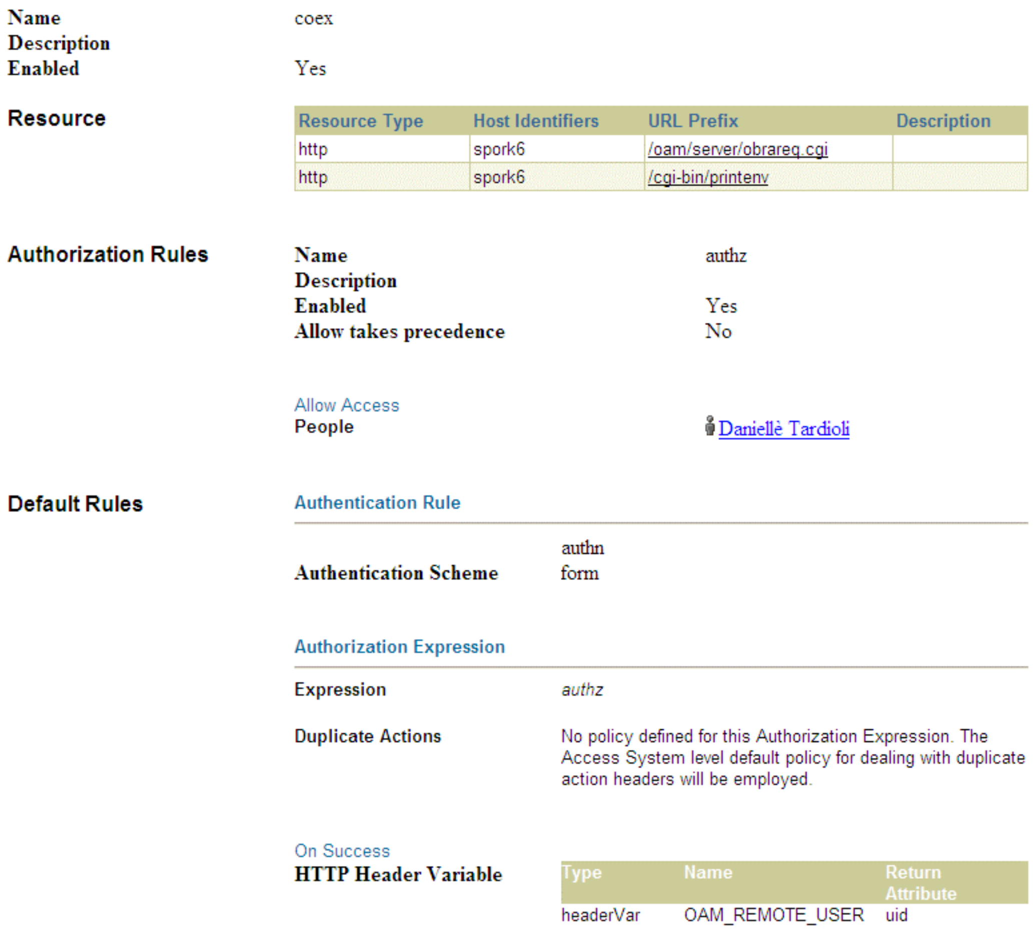
To protect this resource, create an Oracle Access Manager 10*g* policy and do the following:

- 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 16–7 shows a sample policy domain.

Figure 16–7 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

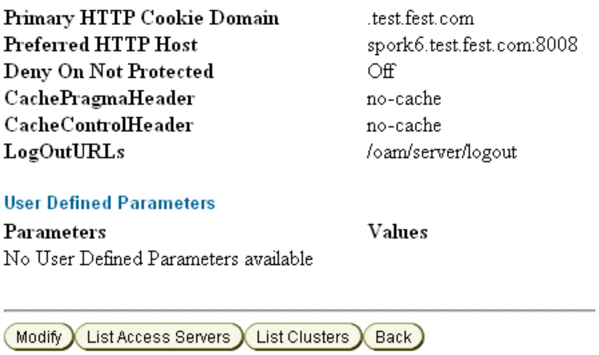
16.12 Configuring Logout Settings

You must configure the logout settings, and make sure that logout works at both the WebGates and the Access Manager 11.1.2.1.0 Server. To do this, complete the following steps:

1. Modify the profile of `WebGate 10`*g*`-2`, and set the value of **LogOutURLs**. This value must be the same as that of the logout end point URL of Access Manager 11.1.2.1.0 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 16–8 shows a sample profile of `WebGate 10`*g*`-2`.

Figure 16–8 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 11.1.2.1.0 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 11.1.2.1.0 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**.

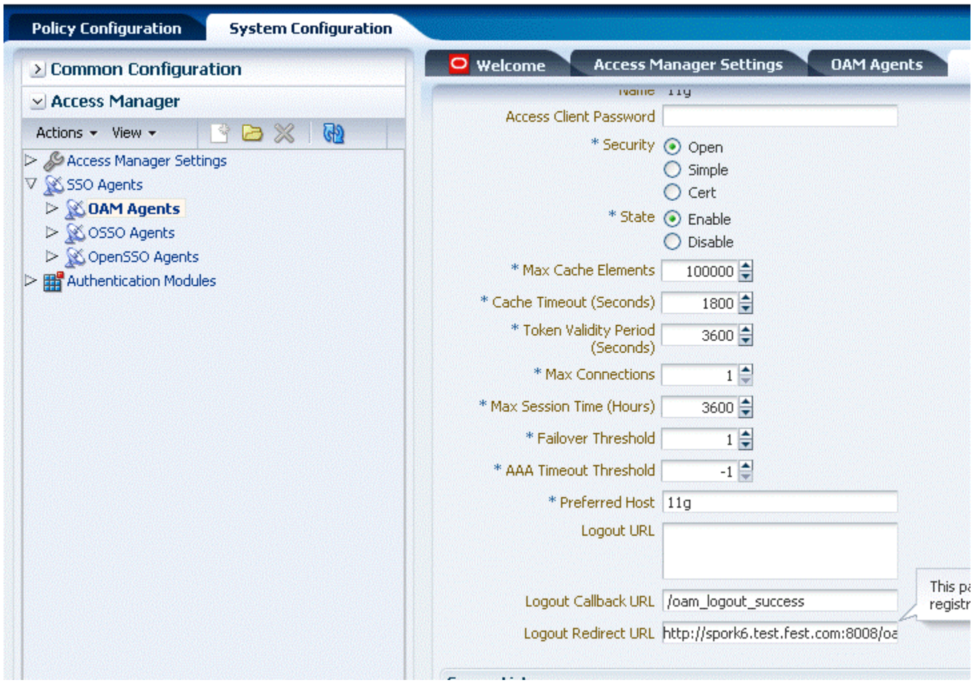
   d. Double-click **OAM Agents**.

   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 16–9 shows the WebGate profile where you must specify the **Logout Redirect URL**.

Figure 16–9 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 11.1.2.1.0 Server. The Access Manager 11.1.2.1.0 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 11.1.2.1.0 server. Access Manager 11.1.2.1.0 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 11.1.2.1.0 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 11.1.2.1.0 server. The Access Manager 11.1.2.1.0 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 11.1.2.1.0 Server. The Access Manager 11.1.2.1.0 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).

16.13 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 11.1.2.1.0 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 11.1.2.1.0 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 11.1.2.1.0 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 11.1.2.1.0 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 11.1.2.1.0 Server, see "Managing Sessions" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.

16.14 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.

17

Coexistence of Sun OpenSSO Enterprise 8.0 with Oracle Access Management Access Manager 11.1.2.1.0

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 (11.1.2.1.0) deployments coexist, after you migrate Sun OpenSSO Enterprise 8.0 to Oracle Access Management Access Manager 11.1.2.1.0.

This chapter contains the following sections:

17.1 Coexistence Overview

During the process of migration from OpenSSO Enterprise 8.0 to Oracle Access Manager 11.1.2.1.0, you can have both OpenSSO Enterprise 8.0 and Access Manager 11.1.2.1.0 deployments coexisting, such that some applications are protected by OpenSSO Enterprise 8.0 while others are protected by Access Manager 11.1.2.1.0. 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.

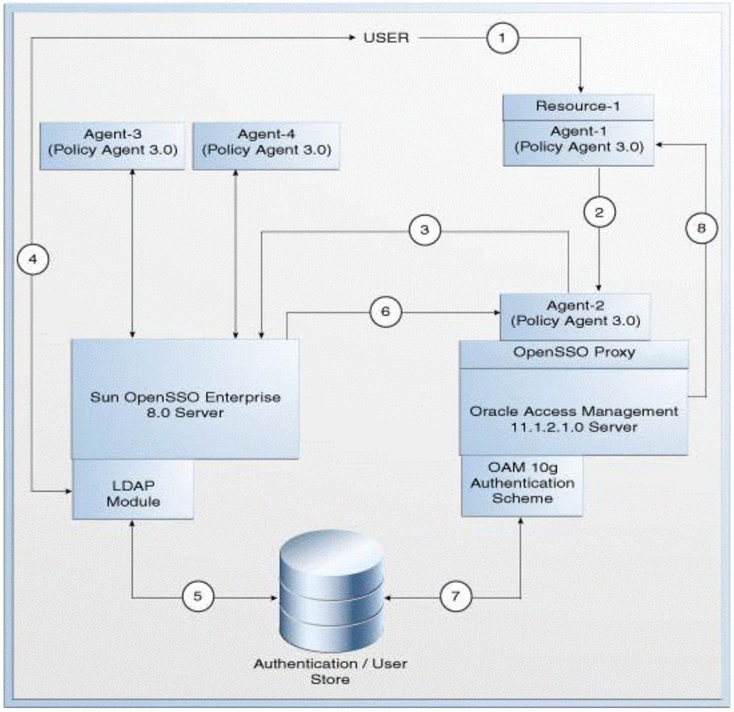
In this mode, Access Manager 11.1.2.1.0 protects the migrated applications and any new applications registered with Access Manager 11*g*; whereas OpenSSO Enterprise 8.0 continues to protect the applications that are not migrated to Access Manager 11.1.2.1.0.

In this coexistence mode, OpenSSO Enterprise 8.0 performs the authentication for all the resources protected by Access Manager 11.1.2.1.0.

17.2 Coexistence Topology

Figure 17–1 illustrates how the authentication is done by the OpenSSO Enterprise 8.0 server when a user requests to access a protected resource.

Figure 17–1 Coexistence of OpenSSO Enterprise 8.0 with Access Manager 11.1.2.1.0



The topology consists of disjoint OpenSSO Enterprise 8.0 and Access Manager 11.1.2.1.0 environments. The numbers 1-8 in the topology show the sequence in which a request flows in the coexistence environment. See Table 17–2 for the request flow.

Topology Description

- `Agent-1`: This is an OpenSSO agent (Policy Agent 3.0) registered with Access Manager 11.1.2.1.0 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 11.1.2.1.0 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 11.1.2.1.0 Server.
- Policy-1: This is the authentication policy created on the Access Manager 11.1.2.1.0 Server for protecting Resource-1. This policy is created as part of the task: Creating an Authentication Policy in Access Manager 11.1.2.1.0 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 11.1.2.1.0 Server Using Agent-2.

Table 17–2 describes the request flow. The numbers in the **Step** column correspond to the numbers in Figure 17–1.

Table 17–1 Request Flow

Step	Description
1	User requests to access Resource-1 which is protected by Agent-1 that communicates with the Access Manager 11.1.2.1.0 Server.
2	Agent-1 redirects the user to the Access Manager 11.1.2.1.0 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 **OAM10gAuthScheme** to assert the user from header **OAM_REMOTE_USER**.
3	The Access Manager 11.1.2.1.0 server end point is protected by Agent-2 that communicates with the OpenSSO Enterprise 8.0 Server. 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 11.1.2.1.0 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 11.1.2.1.0 Server (…./opensso/UI/Login/.....?goto=resource1) after setting the header **OAM_REMOTE_USER** to the **userID** in **Session Attribute Mapping**. The Access Manager 11.1.2.1.0 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 11.1.2.1.0 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. 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.

17.3 Task Roadmap

Table 17–2 lists the steps to configure the coexistence environment.

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	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. Also, create an authentication policy on OpenSSO Enterprise 8.0 to protect the end point URL of the Access Manager 11.1.2.1.0 Server using `Agent-2`.	See, Protecting the End-Point URL of Access Manager 11.1.2.1.0 Server Using Agent-2
4	Configure the data sources for Access Manager 11.1.2.1.0.	See, Configuring Data Source for Access Manager 11.1.2.1.0
5	Update the authentication module in Access Manager 11.1.2.1.0, and point the user identity store to the data source that is configured in Section 17.6.	See, Updating LDAPNoPasswordAuthModule in Access Manager 11.1.2.1.0
6	Create the profile of `Agent-1` in Access Manager 11.1.2.1.0, and install a new Policy Agent 3.0 (Agent-1) pointing to Access Manager 11.1.2.1.0 server.	See, Creating the Profile of Agent-1 in Access Manager 11.1.2.1.0
7	Create an authentication policy in Access Manager 11.1.2.1.0 server to protect `Resource-1`.	See, Creating an Authentication Policy in Access Manager 11.1.2.1.0 to Protect Resource-1

Table 17–2 (Cont.) Tasks to be Completed

Task No	Task	For More Information
8	Change the default cookie name of Access Manager 11.1.2.1.0, so that the cookie names of Access Manager 11.1.2.1.0 and OpenSSO Enterprise 8.0 are different.	See, Modifying the OpenSSO Cookie Name in Access Manager 11.1.2.1.0
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 11.1.2.1.0 Server.	See, Configuring Logout Settings
11	Verify the configuration.	See, Verifying the Configuration

17.4 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 10.7, "Supported Starting Points for Coexistence of Sun OpenSSO Enterprise With Oracle Access Management Access Manager 11.1.2.1.0".

- Ensure that the Sun OpenSSO Enterprise 8.0 and Oracle Access Management Access Manager 11*g* Release 2 (11.1.2.1.0) installations are complete, and the servers are running.

  If you have not installed and configured Oracle Access Management Access Manager 11*g* Release 2 (11.1.2.1.0), 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 (11.1.2.1.0), see "Installing Oracle Identity and Access Management (11.1.2.1.0)" 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 11.1.2.1.0 share the same user store.
- If OpenSSO Enterprise 8.0 and Access Manager 11.1.2.1.0 servers are running on different machines, make sure the time of these machines are synchronized.

17.5 Protecting the End-Point URL of Access Manager 11.1.2.1.0 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 11.1.2.1.0 server. Also, you must create a policy for protecting the end-point URL of the Access Manager 11.1.2.1.0 Server in OpenSSO Enterprise 8.0 Server. To do this, complete the following tasks:

1. Creating Agent-2 Profile for Access Manager 11.1.2.1.0 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 11.1.2.1.0

17.5.1 Creating Agent-2 Profile for Access Manager 11.1.2.1.0 on OpenSSO Enterprise 8.0 Server

Create `Agent-2` profile (as shown in Figure 17–1) 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**.

17.5.2 Installing Agent-2 (Policy Agent 3.0)

Install `Agent-2` (Policy Agent 3.0) in front of the Access Manager 11.1.2.1.0 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*

17.5.3 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 11.1.2.1.0 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 11.1.2.1.0 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 11.1.2.1.0 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.

17.5.4 Creating Authentication Policy on OpenSSO Enterprise 8.0 Server for Access Manager 11.1.2.1.0

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 11.1.2.1.0 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 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 11.1.2.1.0 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**.

17.6 Configuring Data Source for Access Manager 11.1.2.1.0

Configure the data source for Access Manager 11.1.2.1.0 by completing the following steps:

1. Log in to the Oracle Access Manager 11.1.2.1.0 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 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.

17.7 Updating LDAPNoPasswordAuthModule in Access Manager 11.1.2.1.0

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 17.6 as its **User Identity Store**. To do this, complete the following steps:

1. Log in to the Oracle Access Management 11.1.2.1.0 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 console (Administration Server)
   - *`port`* refers to the designated bind port for the Oracle Access Management 11.1.2.1.0 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 17.6.

17.8 Creating the Profile of Agent-1 in Access Manager 11.1.2.1.0

You must create the profile of `Agent-1` in Access Manager 11.1.2.1.0, and install a new Policy Agent 3.0 (`Agent-1`) pointing to Access Manager 11.1.2.1.0 server.

For information about creating the profile of agent in Access Manager 11.1.2.1.0, 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.

17.9 Creating an Authentication Policy in Access Manager 11.1.2.1.0 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 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*.

17.10 Modifying the OpenSSO Cookie Name in Access Manager 11.1.2.1.0

You must change the default cookie name of OpenSSO Cookie in Access Manager 11.1.2.1.0 server to a new name in order to avoid conflict between the cookie names of Access Manager 11.1.2.1.0 and OpenSSO Enterprise 8.0 servers. To do this, complete the following steps:

1. Stop the Access Manager 11.1.2.1.0 Administration Server and the 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, `OAMOpenSSOCookie`).

5. Start the Access Manager 11.1.2.1.0 Administration Server and the 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 11.1.2.1.0 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 console (Administration Server)
   - *port* refers to the designated bind port for the Oracle Access Management 11.1.2.1.0 console, which is the same as the bind port for the Administration Server

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 specify the name of the new cookie name (for example, `OAMOpenSSOCookie`) that you used in step-4, for the field **Cookie Name**.

11. Restart the Access Manager 11.1.2.1.0 Server.

17.11 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 11.1.2.1.0, 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**.

17.12 Configuring Logout Settings

You must configure logout settings to have single logout across OpenSSO Enterprise 8.0 and Access Manager 11.1.2.1.0 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 11.1.2.1.0 Server

17.12.1 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 11.1.2.1.0 Server.

17.12.2 Settings to Initiate Logout from Access Manager 11.1.2.1.0 Server

To initiate logout from the Access Manager 11.1.2.1.0 Server, you must update the **Logout URL** in the respective Policy Agent 3.0 (`Agent-1`) configured with Access Manager 11.1.2.1.0 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 11.1.2.1.0 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 11.1.2.1.0 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.

17.13 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 17–1), 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 11.1.2.1.0 Server, and observe that all the three cookies (**cookie1**, **cookie2**, and **OAM_ID** cookie) are cleared.

18

Coexistence of Sun Java System Access Manager 7.1 with Oracle Access Management Access Manager 11.1.2.1.0

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 (11.1.2.1.0) deployments coexist, after you migrate from Sun Java System Access Manager 7.1 to Access Manager 11.1.2.1.0.

This chapter contains the following sections:

18.1 Coexistence Overview

During the process of migration from Sun Java System Access Manager 7.1 to Oracle Access Manager 11.1.2.1.0, 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 11.1.2.1.0. 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.

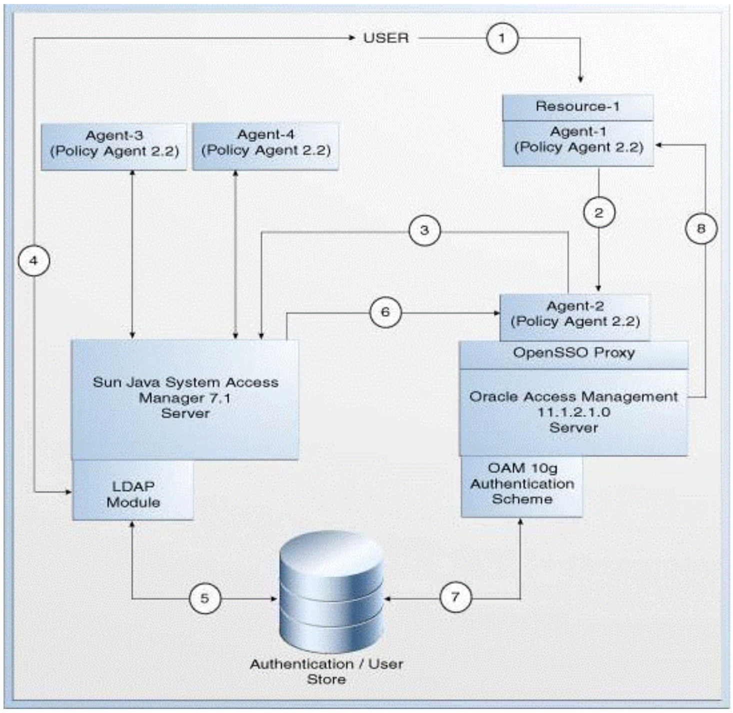
In this mode, Access Manager 11.1.2.1.0 protects the migrated applications and any new applications registered with Access Manager 11.1.2.1.0; whereas Sun Java System Access Manager 7.1 continues to protect the applications that are not migrated to Access Manager 11.1.2.1.0.

In this coexistence mode, Sun Java System Access Manager 7.1 performs the authentication for all the resources protected by Access Manager 11.1.2.1.0.

18.2 Coexistence Topology

Figure 18–1 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 18–1 Coexistence of Sun Java System Access Manager 7.1 with Access Manager 11.1.2.1.0


USER
1
Resource-1
Agent-1 (Policy Agent 2.2)
Agent-3 (Policy Agent 2.2)
Agent-4 (Policy Agent 2.2)
2
3
8
4
6
Agent-2 (Policy Agent 2.2)
OpenSSO Proxy
Sun Java System Access Manager 7.1 Server
Oracle Access Management 11.1.2.1.0 Server
LDAP Module
OAM 10g Authentication Scheme
5
7
Authentication / User Store

The topology consists of disjoint Sun Java System Access Manager 7.1 and Access Manager 11.1.2.1.0 environments. The numbers 1-8 in the topology show the sequence in which a request flows in the coexistence environment. See Table 18–1 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 11.1.2.1.0 Server. You can directly register 2.2 agents in Access Manager 11.1.2.1.0 Server using Remote Registration tool.
- `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 11.1.2.1.0 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 11.1.2.1.0 Server.
- `Policy-1`: This is the policy created on Access Manager 11.1.2.1.0 server for protecting `Resource-1`. This policy is created as part of the task: Creating an Authentication Policy in Access Manager 11.1.2.1.0 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 11.1.2.1.0 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 18–1 describes the request flow. The numbers in the **Step** column correspond to the numbers shown in the topology 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 11.1.2.1.0 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 11.1.2.1.0 Server end point is protected by `Agent-2` that communicates with the Sun Java System Access Manager 7.1 Server. 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 11.1.2.1.0 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 11.1.2.1.0 Server (….`/opensso/UI/Login/.....?goto=resource1`) after setting the header `OAM_REMOTE_USER` to the `userID` in Session Attribute Mapping. The Access Manager 11.1.2.1.0 Server invokes OAM 10g Authentication scheme (**OAM10gAUthScheme**) as per step-2 (`Policy-1`).The Access Manager 11.1.2.1.0 server asserts the user using the header `OAM_REMOTE_USER`, using the **OAM10gScheme** configured for the `Resource-1`.
8	The Access Manager 11.1.2.1.0 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. 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.

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, 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. Also, create a policy on Sun Java System Access Manager 7.1 to protect the end point URL of Access Manager 11.1.2.1.0 Server 11.1.2.1.0 by `Agent-2`.	See, Protecting Access Manager 11g Server's End Point URL by Agent-2
4	Configure the data sources for Access Manager 11.1.2.1.0.	See, Configuring Data Source for Access Manager 11.1.2.1.0
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 18.6.	See, Updating LDAPNoPasswordAuthModule in Access Manager 11g
6	Create the profile of Agent-1 in Access Manager 11.1.2.1.0, and install a new Policy Agent 2.2 (Agent-1) pointing to Access Manager 11.1.2.1.0 server.	See, Creating the Profile of Agent-1 in Access Manager 11.1.2.1.0
7	Create an authentication policy on the Access Manager 11.1.2.1.0 Server to protect `Resource-1`.	See, Creating an Authentication Policy in Access Manager 11.1.2.1.0 to Protect Resource-1

Table 18–2 (Cont.) Tasks to be Completed

Task No	Task	For More Information
8	Change the default cookie name of Access Manager 11.1.2.1.0, so that the cookie names of Access Manager 11*g* and Sun Java System Access Manager 7.1 are different.	See, Modifying the OpenSSO Cookie Name in Access Manager 11.1.2.1.0
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 11.1.2.1.0 Server.	See, Configuring Logout Settings
11	Verify the configuration.	See, Verifying the Configuration

18.4 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 10.8, "Supported Starting Points for Coexistence of Sun Java System Access Manager With Oracle Access Management Access Manager 11.1.2.1.0".

- Ensure that the Sun Java System Access Manager 7.1 and Oracle Access Management Access Manager 11*g* Release 2 (11.1.2.1.0) installations are complete, and the servers are running.

  If you have not installed and configured Oracle Access Management Access Manager 11*g* Release 2 (11.1.2.1.0), 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 (11.1.2.1.0), see "Installing Oracle Identity and Access Management (11.1.2.1.0)" 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 11.1.2.1.0 share the same user store.
- If Sun Java System Access Manager 7.1 and Access Manager 11.1.2.1.0 servers are running on different machines, make sure that the time of these machines are synchronized.

18.5 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 11.1.2.1.0 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

18.5.1 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 18–1) 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**.

18.5.2 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*.

18.5.3 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 11.1.2.1.0 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 11.1.2.1.0 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 11.1.2.1.0 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 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 11.1.2.1.0 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 11.1.2.1.0 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**.

18.6 Configuring Data Source for Access Manager 11.1.2.1.0

Configure the data source for Access Manager 11.1.2.1.0 by completing the following steps:

1. Log in to the Oracle Access Manager 11.1.2.1.0 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 console (administration server).
   - *port* refers to the designated bind port for the Oracle Access Management 11.1.2.1.0 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.

18.7 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 18.6 as its **User Identity Store**. To do this, complete the following steps:

1. Log in to the Oracle Access Management 11.1.2.1.0 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 18.6.

18.8 Creating the Profile of Agent-1 in Access Manager 11.1.2.1.0

You must create the profile of `Agent-1` in Access Manager 11.1.2.1.0 using Remote Registration tool, and install a new Policy Agent 2.2 (`Agent-1`) pointing to Access Manager 11.1.2.1.0 server.

For information about creating the profile of `Agent-1` in Access Manager 11.1.2.1.0, see "Performing Remote Registration for OpenSSO Agents" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.

Note: You can create the profile of Policy Agent 2.2 in Access Manager 11.1.2.1.0 only using the Remote Registration tool.

The following is a sample `OpenSSORequest.xml` file that you will be using in the process of creating the profile of Agent-1 in Access Manager 11.1.2.1.0.

```
<OpenSSORegRequest>

<serverAddress>oam_admin_server_host:oam_admin_server_
port</serverAddress>
<hostIdentifier>2.2_Agent_Name</hostIdentifier>
<agentName>2.2_Agent_Name</agentName>
<agentBaseUrl>web_server_host:web_server_port</agentBaseUrl>
<applicationDomain>2.2_Agent_Name</applicationDomain>
<autoCreatePolicy>true</autoCreatePolicy>
<agentType>WEB</agentType>
<agentVersion>2.2</agentVersion>
<agentDebugDir></agentDebugDir>
<agentAuditDir></agentAuditDir>
<agentAuditFileName></agentAuditFileName>
<protectedAuthnScheme></protectedAuthnScheme>

</OpenSSORegRequest>
```

For information about installing Policy Agent 2.2, see the respective guide in the Sun OpenSSO Enterprise 8.0 Documentation Library.

18.9 Creating an Authentication Policy in Access Manager 11.1.2.1.0 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*.

18.10 Modifying the OpenSSO Cookie Name in Access Manager 11.1.2.1.0

You must change the default cookie name of the Access Manager 11.1.2.1.0 Server to a new name in order to avoid conflict between the cookie names of Access Manager 11.1.2.1.0 and Sun Java System Access Manager 7.1 servers. To do this, complete the following steps:

1. Stop the Access Manager 11.1.2.1.0 Administration Server and the 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 Access Manager 11.1.2.1.0 Administration Server and the 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. Open the `AMAgent.properties file` from the location where you installed `Agent-1`, and do the following based on the type of `Agent-1`.

   - If `Agent-1` is a 2.2 J2EE agent, change the value of the property `com.iplanet.am.cookie.name` to the new cookie name that you have used in step-4 (for example, (`OAMSAMCookie`).

   - If `Agent-1` is a 2.2 Web agent, change the value of the property `com.sun.am.cookie.name` to the new cookie name that you have used in step-4 (for example, `OAMSAMCookie`).

7. Restart the Access Manager 11.1.2.1.0 Server.

18.11 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`.

18.12 Configuring Logout Settings

You must configure logout settings to have single logout across Sun Java System Access Manager 7.1 and Access Manager 11.1.2.1.0 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

18.12.1 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 11.1.2.1.0 server.

18.12.2 Settings to Initiate Logout from Access Manager 11*g* Server

To initiate logout from the Access Manager 11.1.2.1.0 server, you must update the **Logout URL** in the respective Policy Agent 2.2 (`Agent-1`) configured with Access Manager 11.1.2.1.0 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 11.1.2.1.0 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`

18.13 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 18–1), 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 11.1.2.1.0 Server, and observe that all the three cookies (**cookie1**, **cookie2**, and **OAM_ID** cookie) are cleared.