Oracle® Fusion Middleware

Migration Guide for Oracle Identity and Access Management

11*g* Release 2 (11.1.2.2.0)

E49917-04

September 2014

Documentation for Oracle Fusion Middleware administrators who wish to migrate to Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0).

ORACLE

Oracle Fusion Middleware Migration Guide for Oracle Identity and Access Management, 11*g* Release 2 (11.1.2.2.0)

E49917-04

Primary Author: Shynitha K S

Contributors: Allison Sparshott, Ankit Mittal, 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, Sharadchandra Chavali, Sitaraman Swaminathan, Sree Chitturi, Srinivas Nagandla, Stephen Mathew, Steven Frehe, Stuart Duggan, Svetlana Kolomeyskaya, Sylaja Kannan, Tushar Wagh, Umesh Waghode, Vadim Lander, Vishal Mishra, Venu Shastri, William Cai, Wortimla Rs

Contents

3 Migrating Oracle Adaptive Access Manager 10*g* Environments

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

5 Migrating Sun OpenSSO Enterprise 8.0 Environments

6 Migrating Sun Java System Access Manager 7.1 Environments

Preface

This document describes how to migrate to Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0) components.

Audience

This document is intended for administrators who are responsible for migrating existing Identity Management environments to Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0).

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 (11.1.2.2.0) documentation library:

- *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*
- *Oracle Fusion Middleware Upgrade 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:

1

Introduction to Oracle Identity and Access Management Migration and Coexistence

This chapter provides an overview of Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0) product and the documentation roadmap. This chapters also describes the supported migration and coexistence scenarios for 11.1.2.1.0.

This chapter includes the following topics:

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 (11.1.2.2.0) includes the following products:

- 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 Manager
- Oracle Entitlements Server
- Oracle Privileged Account Manager
- Oracle Identity Navigator

1.2 Migration and Coexistence Scenarios

The term **Migration** refers to the migration of 10*g* version of Oracle Identity and Access Management component or Sun products to Oracle Identity and Access Management 11.1.2.2.0, scenarios where you migrate the following products to Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0). In these migration scenarios, you must install a new 11*g* Release 2 (11.1.2.2.0) Oracle Home (*IAM_HOME* or *ORACLE_HOME*) and then migrate your configuration data from your previous installation to the new 11*g* Release 2 (11.1.2.2.0) 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
- Oracle Identity Analytics

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 11.1.2.2.0 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 11.1.2.2.0 Servers.

The following are the coexistence scenarios supported in 11*g* Release 2 (11.1.2.2.0):

- Coexistence of Oracle Access Manager 10*g* with Oracle Access Management Access Manager 11.1.2.2.0
- Coexistence of Sun OpenSSO Enterprise 8.0 with Oracle Access Management Access Manager 11.1.2.2.0
- Coexistence of Sun Java System Access Manager 7.1 with Oracle Access Management Access Manager 11.1.2.2.0

> **Note:** This guide covers the procedures for all the migration and coexistence scenarios described in this section.

1.3 Upgrade Scenarios

The term **Upgrade** refers to the upgrade of existing Oracle Identity and Access Management 11*g* Release 1 and 11*g* Release 2 components to Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0). For each of these upgrade scenarios, you use the Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0) installer to update your existing Oracle Home (*IAM_HOME*) to Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0).

You can upgrade the following Oracle Identity and Access Management components to Oracle Identity and Access Management 11.1.2.2.0:

- Oracle Identity and Access Management 11*g* Release 2 (11.1.2.1.0) Components

  - Oracle Access Manager 11.1.2.1.0
  - Oracle Adaptive Access Manager 11.1.2.1.0
  - Oracle Identity Manager 11.1.2.1.0
  - Oracle Entitlements Server 11.1.2.1.0
  - Oracle Privileged Account Manager 11.1.2.1.0
  - Oracle Identity Navigator 11.1.2.1.0
- Oracle Identity and Access Management 11*g* Release 2 (11.1.2) Components
  - Oracle Access Manager 11.1.2
  - Oracle Adaptive Access Manager 11.1.2
  - Oracle Identity Manager 11.1.2
  - Oracle Entitlements Server 11.1.2
  - Oracle Privileged Account Manager 11.1.2
  - Oracle Identity Navigator 11.1.2
- Oracle Identity and Access Management 11*g* Release 1 (11.1.1.7.0) Components
  - Oracle Access Manager 11.1.1.7.0
  - Oracle Adaptive Access Manager 11.1.1.7.0
  - Oracle Identity Manager 11.1.1.7.0
  - Oracle Identity Navigator 11.1.1.7.0
- Oracle Identity and Access Management 11*g* Release 1 (11.1.1.5.0) Components
  - 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 9.1.x.x

Note: This guide covers only the migration and coexistence scenarios described in Section 1.2, "Migration and Coexistence Scenarios".

The upgrade scenarios are covered in the *Oracle Fusion Middleware Upgrade Guide for Oracle Identity and Access Management*.

1.4 Supported Starting Points for Migration and Coexistence

This section describes the supported starting points for Oracle Identity and Access Management migration and coexistence.

This section contains the following sub-sections:

- Supported Starting Points for Oracle Access Manager 10g Migration
- Supported Starting Points for Oracle Single Sign-On 10g Migration
- Supported Starting Points for Sun OpenSSO Enterprise Migration

- Supported Starting Points for Sun Java System Access Manager Migration
- Supported Starting Points for Oracle Identity Analytics Migration
- Supported Starting Points for Coexistence of Oracle Access Manager 10g With Oracle Access Management Access Manager 11.1.2.2.0
- Supported Starting Points for Coexistence of Sun OpenSSO Enterprise With Oracle Access Management Access Manager 11.1.2.2.0
- Supported Starting Points for Coexistence of Sun Java System Access Manager With Oracle Access Management Access Manager 11.1.2.2.0

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

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

Table 1–1 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.

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

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

Table 1–2 Oracle Adaptive Access Manager 10g Releases Supported for Migration

Release	Description
Oracle Adaptive Access Manager 10*g* (10.1.4.5.0)	This version of Oracle Adaptive Access Manager is supported for migration.

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

Table 1–3 lists the releases of Oracle Single Sign-On 10*g* supported for migration.

Table 1–3 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).

1.4.4 Supported Starting Points for Sun OpenSSO Enterprise Migration

Table 1–4 lists the releases of Sun OpenSSO Enterprise supported for migration.

Table 1–4 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.

1.4.5 Supported Starting Points for Sun Java System Access Manager Migration

Table 1–5 lists the releases of Sun Java System Access Manager supported for migration.

Table 1–5 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.

1.4.6 Supported Starting Points for Oracle Identity Analytics Migration

Table 1–6 lists the releases of Oracle Identity Analytics supported for migration.

Table 1–6 Oracle Identity Analytics Releases Supported for Migration

Release	Description
Oracle Identity Analytics 11*g* Release 1 (11.1.1.5.0)	This version of Oracle Identity Analytics is supported for migration.

1.4.7 Supported Starting Points for Coexistence of Oracle Access Manager 10*g* With Oracle Access Management Access Manager 11.1.2.2.0

Table 1–7 lists the releases of Oracle Access Manager 10*g* supported for coexistence with Oracle Access Management Access Manager 11*g* Release 2 (11.1.2.2.0).

Table 1–7 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 (11.1.2.2.0) deployments coexist.

1.4.8 Supported Starting Points for Coexistence of Sun OpenSSO Enterprise With Oracle Access Management Access Manager 11.1.2.2.0

Table 1–8 lists the releases of Sun OpenSSO Enterprise supported for coexistence with Oracle Access Management Access Manager 11*g* Release 2 (11.1.2.2.0).

Table 1–8 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 (11.1.2.2.0) deployments coexist.

1.4.9 Supported Starting Points for Coexistence of Sun Java System Access Manager With Oracle Access Management Access Manager 11.1.2.2.0

Table 1–9 lists the releases of Sun Java System Access Manager supported for coexistence with Oracle Access Management Access Manager 11*g* Release 2 (11.1.2.2.0).

Table 1–9 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.

1.5 Documentation Roadmap

This section provides the documentation roadmap for all the migration and coexistence scenarios.

Table 1–10 lists all the migration and coexistence scenarios, and the chapters in which the respective migration and coexistence procedure is described. Depending on the migration and coexistence scenario, go to the respective chapter, and follow the procedure.

Table 1–10 Documentation Roadmap for Oracle Identity and Access Management Migration and Coexistence

Scenarios	Chapter
Migration Scenarios	
Oracle Access Manager 10*g* to Oracle Access Management Access Manager 11.1.2.2.0 migration	Chapter 2, "Migrating Oracle Access Manager 10g Environments"
Oracle Adaptive Access Manager 10*g* to Oracle Adaptive Access Manager 11.1.2.2.0 migration	Chapter 3, "Migrating Oracle Adaptive Access Manager 10g Environments"
Oracle Single Sign-On 10*g* to Oracle Access Management Access Manager 11.1.2.2.0 migration	Chapter 4, "Migrating Oracle Single Sign-On 10g Environments"
Sun OpenSSO Enterprise 8.0 to Oracle Access Management Access Manager 11.1.2.2.0 migration	Chapter 5, "Migrating Sun OpenSSO Enterprise 8.0 Environments"
Sun Java System Access Manager 7.1 to Oracle Access Management Access Manager 11.1.2.2.0 migration	Chapter 6, "Migrating Sun Java System Access Manager 7.1 Environments"
Oracle Identity Analytics 11.1.1.5.0 to Oracle Identity Manager 11.1.2.2.0 migration	Chapter 7, "Migrating Completed Certifications From Oracle Identity Analytics to Oracle Identity Manager"
Coexistence Scenarios	
Coexistence of Oracle Access Manager 10*g* with Oracle Access Management Access Manager 11.1.2.2.0	Chapter 8, "Coexistence of Oracle Access Manager 10g with Oracle Access Management Access Manager 11.1.2.2.0"
Coexistence of Sun OpenSSO Enterprise 8.0 with Oracle Access Management Access Manager 11.1.2.2.0	Chapter 9, "Coexistence of Sun OpenSSO Enterprise 8.0 with Oracle Access Management Access Manager 11.1.2.2.0"

Table 1–10 (Cont.) Documentation Roadmap for Oracle Identity and Access Management Migration and Coexistence

Scenarios	Chapter
Coexistence of Sun Java System Access Manager 7.1 with Oracle Access Management Access Manager 11.1.2.2.0	Chapter 10, "Coexistence of Sun Java System Access Manager 7.1 with Oracle Access Management Access Manager 11.1.2.2.0"

Part II

Migrating to Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0)

This part includes the following chapters:

2

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 (11.1.2.2.0).

This chapter contains the following sections:

2.1 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 11.1.2.2.0.

- Host identifiers

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

During this migration, you must install Access Manager 11*g* Release 2 (11.1.2.2.0), 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 (11.1.2.2.0) Oracle Home.

This section contains the following topics:

2.1.1 Modes of Migration

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

2.1.1.1 Complete Migration

This mode of migration migrates all artifacts of Oracle Access Manager 10*g*, which are compatible with 11.1.2.2.0, to Access Manager 11.1.2.2.0. 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.

2.1.1.2 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 11.1.2.2.0. 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 11.1.2.2.0 environment. If an artifact that you wish to migrate is already present in the Access Manager 11.1.2.2.0 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.

2.1.1.3 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 11.1.2.2.0 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 web page, when you modify any policy related artifact using the Oracle Access Manager 10*g* Policy Manager console.

2.1.2 Migration Summary

Table 2–1 summarizes the artifacts of Oracle Access Manager 10*g* that can be migrated to Access Manager 11.1.2.2.0:

Table 2–1 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 11.1.2.2.0. ■ Host name variations in Oracle Access Manager 10*g*, which contain non-numeric characters in the port values, are not migrated to Access Manager 11.1.2.2.0. 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. ■ If a resource in Oracle Access Manager 10*g* policy data is not associated with host identifier, then migration tool creates host identifier called `OAM11G_GLOBAL_HOSTID` in Access Manager 11.1.2.2.0 during migration, and associates the resource with the newly created host identifier. This is because resource cannot be created without host identifier in Access Manager 11.1.2.2.0. Post migration, you must add appropriate host name variation in the host identifier for all those resources that did not have host identifier in Oracle Access Manager 10*g* policy data.
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 11.1.2.2.0 server depending to the security mode of the WebGates. For more information, see Section 2.7, "Configuring Transport Security Mode for Access Manager 11.1.2.2.0 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 2–4. ■ 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 11.1.2.2.0 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 11.1.2.2.0. 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.

Table 2–1 (Cont.) Compatibility of Artifacts

Artifact	Description
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 11.1.2.2.0. Therefore, external authentication schemes are migrated to 11.1.2.2.0 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 11.1.2.2.0.
Resource Types	■ Oracle Access Manager 10*g* resource types and the migrated Access Manager 11.1.2.2.0 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 11.1.2.2.0.

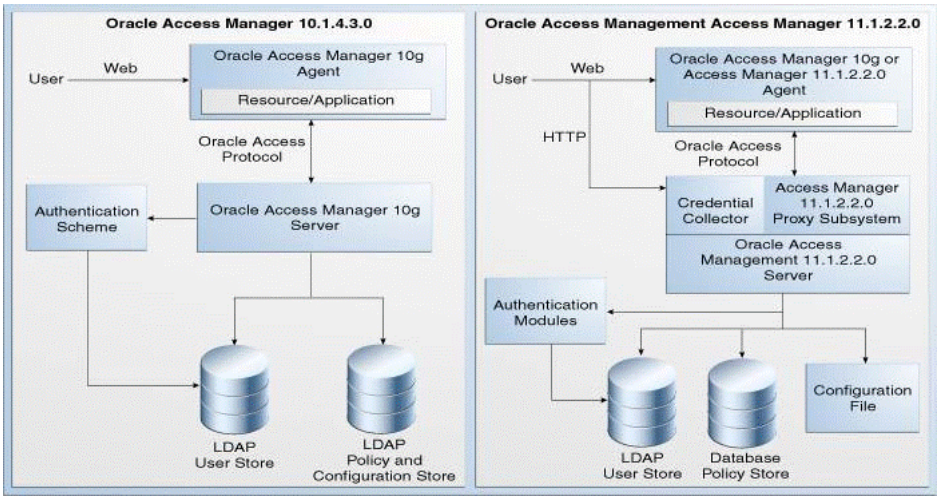
Table 2–1 (Cont.) Compatibility of Artifacts

Artifact	Description
Policy Domains	■ Policy domains of Oracle Access Manager 10*g* map to a distinct application domain in Access Manager 11.1.2.2.0. ■ URL prefixes are migrated to Access Manager 11.1.2.2.0. 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 11.1.2.2.0 does not support them. For authentication rules, both the success and failure redirects and responses are migrated to Access Manager 11.1.2.2.0. 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 11.1.2.2.0: ■ 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 11.1.2.2.0. ■ 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.

2.2 Topology Comparison

Figure 2–1 compares the topologies of Oracle Access Manager 10g and Access Manager 11.1.2.2.0.

Figure 2–1 Comparison of Oracle Access Manager 10g and Access Manager 11.1.2.2.0 Topologies



2.3 Migration Roadmap

Table 2–2 lists the steps to migrate Oracle Access Manager 10*g* to Access Manager 11.1.2.2.0.

Table 2–2 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 (11.1.2.2.0).	See, Installing Oracle Identity and Access Management 11.1.2.2.0
3	Configure Access Manager 11.1.2.2.0.	See, Configuring Oracle Access Management Access Manager 11.1.2.2.0
4	Configure the security mode of the Access Manager 11.1.2.2.0 server instance and the WebGates, so that the Access Manager 11.1.2.2.0 server accepts connections from the agents when WebGates start communicating with Access Manager 11.1.2.2.0 after migration.	See, Configuring Transport Security Mode for Access Manager 11.1.2.2.0 Server
5	Start the Administration Server and the Access Manager 11.1.2.2.0 Managed Servers.	See, Starting Administration Server and Access Manager 11.1.2.2.0 Managed Server(s)

Table 2–2 (Cont.) Migration Tasks

Task No	Task	For More Information
6	Create a properties file with the LDAP details and the required information.	See, Creating the Properties File
7	Generate the assessment report, and analyze what agents and artifacts can be migrated to Access Manager 11.1.2.2.0. 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 11.1.2.2.0.	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 11.1.2.2.0.	See, Migrating the Artifacts of Oracle Access Manager 10g to Access Manager 11.1.2.2.0
11	If you are using 10*g* WebGates with Access Manager 11.1.2.2.0, you must configure the centralized logout for 10*g* WebGates to work with Access Manager 11.1.2.2.0 server.	See, Configuring Centralized Logout for 10g WebGates with Access Manager 11.1.2.2.0
12	Associate the migrated WebGates with the Oracle Access Management 11.1.2.2.0 Server.	See, Associating the WebGates with Access Manager 11.1.2.2.0 Server
13	Verify the migration.	See, Verifying the Migration

2.4 Prerequisites for Migration

You must complete the following prerequisites for migrating Oracle Access Manager 10*g* to Access Manager 11.1.2.2.0:

1. Read the system requirements and certification documents to ensure that your environment meets the minimum requirements for the products you are installing.
   - *Oracle Fusion Middleware System Requirements and Specifications*

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

- *Oracle Fusion Middleware Supported System Configurations*

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

- For interoperability and compatibility issues that may arise when installing, refer to *Oracle Fusion Middleware Interoperability and Compatibility Guide*.

  This document contains important information regarding the ability of Oracle Fusion Middleware products to function with previous versions of other Oracle Fusion Middleware, Oracle, or third-party products. This information is applicable to both new Oracle Fusion Middleware users and existing users who are upgrading their existing environment.

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 1.4, "Supported Starting Points for Migration and Coexistence".
3. Make sure that all the user stores configured in your Oracle Access Manager 10*g* deployment are running.

2.5 Installing Oracle Identity and Access Management 11.1.2.2.0

As part of the migration process, you must install Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0). Oracle Identity and Access Management is a suite that contains Oracle Access Management Access Manager 11.1.2.2.0. 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 11.1.2.2.0, see "Installing Oracle Identity and Access Management (11.1.2.2.0)" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

2.6 Configuring Oracle Access Management Access Manager 11.1.2.2.0

After installing Oracle Identity and Access Management 11.1.2.2.0, you must configure Access Manager 11.1.2.2.0, and create a domain.

For information about configuring Access Manager 11.1.2.2.0, see "Configuring Oracle Access Management" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

2.7 Configuring Transport Security Mode for Access Manager 11.1.2.2.0 Server

You must configure the security mode of the Access Manager 11.1.2.2.0 Server, so that the migrated WebGates communicate with the Access Manager 11.1.2.2.0 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 11.1.2.2.0 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:

2.7.1 Deciding the Security Mode of Access Manager 11.1.2.2.0 Server

If all the WebGates that you migrate have the same security mode, you must configure the Access Manager 11.1.2.2.0 Server in the respective modes. If you have mix of migrated WebGates configured in different security modes, you must configure the Access Manager 11.1.2.2.0 Server in the mode with the lower security level. Table 2–3 lists the various use cases and the security mode in which you must configure the Access Manager 11.1.2.2.0 Server.

Table 2–3 Choosing the Security Mode for Access Manager 11.1.2.2.0 Server

Transport Security Mode of Oracle Access Manager 10*g* WebGates	Security Mode to be Configured for Access Manager 11.1.2.2.0 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 11.1.2.2.0 Server.
All `Simple`	`Simple`	See Configuring Simple Mode Communication for Access Manager 11.1.2.2.0 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 11.1.2.2.0 Server.

2.7.2 Configuring Cert Mode Communication for Access Manager 11.1.2.2.0 Server

To configure `Cert` mode communication for Access Manager 11.1.2.2.0, 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 11.1.2.2.0 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 11.1.2.2.0 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 11.1.2.2.0 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.

2.7.3 Configuring Simple Mode Communication for Access Manager 11.1.2.2.0 Server

To configure `Simple` mode communication for the Access Manager 11.1.2.2.0 Server, complete the following steps:

1. Log in to the Oracle Access Management 11.1.2.2.0 Administration console, using the following URL:

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

   where `<host>` is the machine on which Access Manager 11.1.2.2.0 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.

2.8 Starting Administration Server and Access Manager 11.1.2.2.0 Managed Server(s)

Before you start migrating Oracle Access Manager 10*g* to Access Manager 11.1.2.2.0, make sure that the WebLogic Administration Server and the Access Manager 11.1.2.2.0 Managed Servers are up and running. For information about starting the Administration Server and the Managed Server(s), see Appendix A.2, "Starting the Servers".

2.9 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 2–4 describes the values you must provide for each of the properties in the properties file.

Table 2–4 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 2–4 (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.

Table 2–4 (Cont.) Property File Values

Property	Description
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 #.
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 11.1.2.2.0 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 11.1.2.2.0, 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 11.1.2.2.0. 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 2–4 (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 11.1.2.2.0. 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 11.1.2.2.0, compatible with less features in Access Manager 11.1.2.2.0, and the artifacts that are ignored in Access Manager 11.1.2.2.0. 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 11.1.2.2.0, incompatible in Access Manager 11.1.2.2.0, compatible with less features in Access Manager 11.1.2.2.0, and the artifacts that are ignored in Access Manager 11.1.2.2.0. For more information about the artifacts that are incompatible, and compatible with less features, see Table 2–6.
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 2–4 (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 11.1.2.2.0. 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 11.1.2.2.0. 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 10*g*_*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 10*g*_*Installation_Directory*/Access/oblix/config/ldap/WebResrcDB.xml file.

2.10 Generating the Assessment Report

You should generate an assessment report before you can migrate the Oracle Access Manager 10*g* artifacts to Access Manager 11.1.2.2.0.

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 11.1.2.2.0.

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 11.1.2.2.0
3. Detailed information about all the artifacts of Oracle Access Manager 10*g* in a tabular format.

Table 2–5 lists the columns of the table, which displays information about the artifacts of Oracle Access Manager 10*g*:

Table 2–5 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 2–5 (Cont.) Assessment Report Content

Column No	Column	Description
4	**COMPATIBILITY**	This column displays information about the compatibility of artifacts in Access Manager 11.1.2.2.0.if the artifact is compatible with Access Manager 11.1.2.2.0 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 11.1.2.2.0 and the migration utility does not perform any additional modelling. ▪ **INCOMPATIBLE**: This indicates that the artifact is not supported in Access Manager 11.1.2.2.0, and will not be migrated. ▪ **COMPATIBLE_WITH_LESS_FEATURES**: This indicates that the artifact is compatible in Access Manager 11.1.2.2.0, but with less features. The migration utility performs some modelling in order to map this artifact to 11.1.2.2.0. All the artifacts with this compatibility mode are migrated. ▪ **IGNORE**: This indicates that the artifact is not useful in Access Manager 11.1.2.2.0, 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 11.1.2.2.0.

Table 2–6 shows the types of artifacts of Oracle Access Manager 10*g* that are incompatible and compatible with less features in Access Manager 11.1.2.2.0.

Table 2–6 Assessment Reports Summary

Artifacts	Description
INCOMPATIBLE	▪ Policy domains that contain URL prefixes for heterogeneous resource types are incompatible with the Access Manager 11.1.2.2.0 environment. ▪ Operation **OTHER** for type HTTP is incompatible with Access Manager 11.1.2.2.0, 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 2–6 (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 11.1.2.2.0 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 11.1.2.2.0. The other conditions such as **Months of the Year** and **Days of the Month** are not supported in Access Manager 11.1.2.2.0, 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 2.9, "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 2.13, "Migrating the Artifacts of Oracle Access Manager 10g to Access Manager 11.1.2.2.0".

    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 2.13, "Migrating the Artifacts of Oracle Access Manager 10g to Access Manager 11.1.2.2.0".

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".

2.11 Restarting the Administration Server

Restart the WebLogic Administration Server for the domain with Access Manager 11.1.2.2.0 by doing the following:

1. Stop the WebLogic Administration Server.
2. Start the WebLogic Administration Server.

For information about stopping Administration Server, see Appendix A.1.2, "Stopping the WebLogic Administration Server".

For information about starting Administration Server, see Appendix A.2.1, "Starting the WebLogic Administration Server".

2.12 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 2.9, "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.

2.13 Migrating the Artifacts of Oracle Access Manager 10*g* to Access Manager 11.1.2.2.0

Before you migrate Oracle Access Manager 10*g* to Access Manager 11.1.2.2.0, it is recommended that you generate an assessment report (as described in Section 2.10, "Generating the Assessment Report"), and analyze what artifacts are compatible and incompatible in Access Manager 11.1.2.2.0.

Note: If you decide to migrate Oracle Access Manager 10*g* to Access Manager 11.1.2.2.0 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 2.12, "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 11.1.2.2.0:

```
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.

2.14 Configuring Centralized Logout for 10*g* WebGates with Access Manager 11.1.2.2.0

If you are using 10*g* WebGates with Access Manager 11.1.2.2.0, you must configure the centralized logout settings for 10*g* WebGates to work with Access Manager 11.1.2.2.0 server, after migrating Oracle Access Manager 10*g* to Access Manager 11.1.2.2.0.

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 11.1.2.2.0.

2.15 Associating the WebGates with Access Manager 11.1.2.2.0 Server

After you migrate Oracle Access Manager 10*g* to Access Manager 11.1.2.2.0, you must associate all of the migrated WebGates with the Access Manager 11.1.2.2.0 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 11.1.2.2.0 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 11.1.2.2.0 Server instance is running.

      Port: Specify the proxy port for Access Manager 11.1.2.2.0 Server instance. The default proxy port for Access Manager 11.1.2.2.0 is `5575`.

      Transport Security: Specify the same transport security mode as that of the Access Manager 11.1.2.2.0 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 11.1.2.2.0 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 11.1.2.2.0 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 11.1.2.2.0 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 11.1.2.2.0 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 11.1.2.2.0 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 11.1.2.2.0 Server. If you restart the web server that hosts the WebGate, WebGate starts talking to the Access Manager 11.1.2.2.0 server immediately.
   - Increase the value of the parameter `MAX Connections` by one, so that the WebGate establishes the connection with Access Manager 11.1.2.2.0 server. If the load on WebGate is more, it takes less time to connect to the Access Manager 11.1.2.2.0 Server.

   WebGate now gets the new configuration information from the Access Manager 11.1.2.2.0 Server, which has only one primary server. Thus, the WebGate communicates only with the Access Manager 11.1.2.2.0 server. Once this is done, you can reduce the value of `MAX Connections` as there is only one server.

2.16 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 11.1.2.2.0 is running, and *port* is the port number.

   Verify that the Oracle Access Manager 10*g* artifacts are migrated to Access Manager 11.1.2.2.0.

> **Note:** This completes the migration. For more information on managing the Oracle Access Management Access Manager 11.1.2.2.0, see *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.

2.17 Troubleshooting

This section describes solutions to the common problems that you might encounter when migration Oracle Access Manager 10*g* to Access Manager 11.1.2.2.0. 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
- LDAP Paging Feature of Oracle Access Manager Migration May Not Work

2.17.1 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**.

2.17.2 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
   ```

2.17.3 LDAP Paging Feature of Oracle Access Manager Migration May Not Work

With some directories or special configurations, the LDAP paging feature of Oracle Access Manager 10*g* migration may not work. In such situations, disable the LDAP paging by adding the property `enable_ldap_paging` in the `oam_migration.properties` file that you created in Section 2.9, "Creating the Properties File", and setting the value of this property to `false`.

When the property `enable_ldap_paging` is set to `false`, migration tool fetches all LDAP entries at once. When this property is set to `false` and if data size is large, it is recommended that you increase the heap size for Oracle Access Manager Administration Server process.

3

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 (11.1.2.2.0).

This chapter contains the following sections:

3.1 Migration Overview

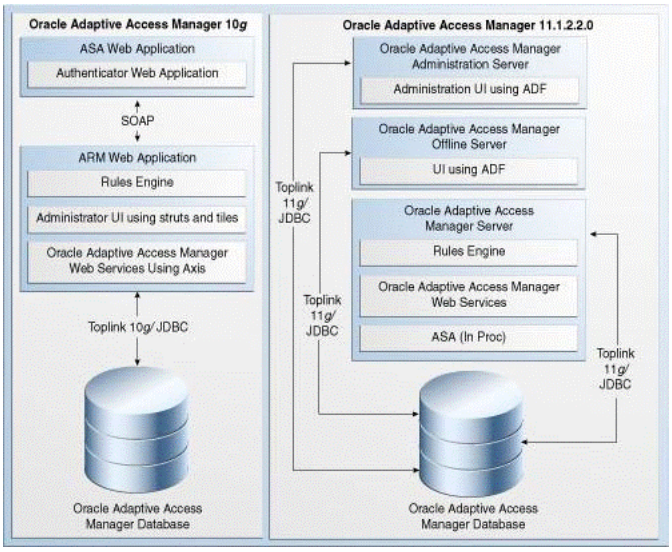
The process for migrating OAAM 10*g* to OAAM 11.1.2.2.0 involves installing Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0), configuring OAAM 11.1.2.2.0, upgrading OAAM 10*g* schemas, configuring the database security store, and upgrading the Oracle Adaptive Access Manager middle tier.

For more information about other migration scenarios, see Section 1.2, "Migration and Coexistence Scenarios".

3.2 Topology Comparison

Figure 3–1 compares the topologies of OAAM 10*g* and OAAM 11.1.2.2.0.

Figure 3–1 Comparison of OAAM 10g and OAAM 11g Topologies



3.3 Migration Roadmap

Table 3–1 provides the migration roadmap.

Table 3–1 Task Roadmap

Task No	Task	For More Information
1	Complete the prerequisites.	See, Prerequisites for Migration
2	Install Oracle Identity and Access Management 11.1.2.2.0.	See, Installing Oracle Identity and Access Management 11.1.2.2.0
3	Create Oracle Platform Security Services (OPSS) schema, and Metadata Services (MDS) schema using Repository Creation Utility (RCU).	See, Creating Oracle Platform Security Services Schema
4	Upgrade the OAAM 10*g* schema using the Upgrade Assistant.	See, Upgrading OAAM 10g Schema
5	Configure OAAM 11.1.2.2.0 in a new or existing domain.	See, Configuring OAAM 11.1.2.2.0 in a New or Existing Oracle WebLogic Domain
6	Configure the database security store by running the `configuresecuritystore.py` script.	See, Configuring Database Security Store

Table 3–1 (Cont.) Task Roadmap

Task No	Task	For More Information
7	Configure the Node Manager.	See, Configuring Node Manager
8	Start the WebLogic Administration Server.	See, Starting WebLogic Administration Server
9	Stop the OAAM Managed Servers (OAAM Admin Server, OAAM Server, and OAAM Offline Server).	See, Stopping OAAM Managed Servers
10	Upgrade the OAAM middle tier using Upgrade Assistant.	See, Upgrading OAAM Middle Tier Using Upgrade Assistant
11	Start the OAAM Managed Servers (OAAM Admin Server, OAAM Server, and OAAM Offline Server).	See, Starting OAAM Managed Servers
12	Verify the migration.	See, Verifying the Migration

3.4 Prerequisites for Migration

You must complete the following prerequisites for migrating Oracle Adaptive Access Manager 10*g* to Oracle Adaptive Access Manager 11.1.2.2.0:

1. Read the system requirements and certification documents to ensure that your environment meets the minimum requirements for the products you are installing.

   - *Oracle Fusion Middleware System Requirements and Specifications*

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

   - *Oracle Fusion Middleware Supported System Configurations*

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

   - For interoperability and compatibility issues that may arise when installing, refer to *Oracle Fusion Middleware Interoperability and Compatibility Guide*.

     This document contains important information regarding the ability of Oracle Fusion Middleware products to function with previous versions of other Oracle Fusion Middleware, Oracle, or third-party products. This information is applicable to both new Oracle Fusion Middleware users and existing users who are upgrading their existing environment.

Note: For information about Oracle Fusion Middleware concepts and directory structure, see "Understanding Oracle Fusion Middleware Concepts and Directory Structure" in the *Oracle Fusion Middleware Installation Planning Guide for Oracle Identity and Access Management*.

---

2. Verify that the Oracle Adaptive Access Manager 10*g* version that you are using is supported for migration. For information about supported starting points for Oracle Adaptive Access Manager 10*g* migration, see Section 1.4.2, "Supported Starting Points for Oracle Adaptive Access Manager 10g Migration".

3. If you wish to upgrade oaam_offline server 10*g* to 11.1.2.2.0 and if you have scheduled load jobs that load from `oaam_server` 10*g* schema, then you must upgrade `oaam_server` before you can start oaam_offline server (as described in Section 3.14, "Starting OAAM Managed Servers"). If you cannot upgrade `oaam_server` schema, then you must run the following SQL statement to create the view in the `oaam_server` schema:

```
create or replace view oaam_load_data_view as
select l.create_time LOGIN_TIMESTAMP, l.request_id SESSION_ID,
l.user_id USER_ID, l.user_login_id LOGIN_ID, l.node_id DEVICE_ID,
l.user_group_id GROUP_ID, l.remote_ip_addr IP_ADDRESS,
l.auth_status AUTH_STATUS, l.auth_client_type_code CLIENT_TYPE,
(SELECT t1.data_value FROM v_fprints t1
WHERE t1.fprint_id=l.fprint_id) USER_AGENT,
(SELECT t2.data_value FROM v_fprints t2
WHERE t2.fprint_id=l.digital_fp_id) FLASH_FINGERPRINT,
l.sent_dig_sig_cookie DIGITAL_COOKIE,
l.expected_dig_sig_cookie EXP_DIGITAL_COOKIE,
l.sent_secure_cookie SECURE_COOKIE,
l.expected_secure_cookie EXP_SECURE_COOKIE
from vcrypt_tracker_usernode_logs l;
```

Note: You can run the following SQL statement to list all the OAAM schemas in a database with their version numbers:

```
SELECT OWNER, VERSION FROM SCHEMA_VERSION_REGISTRY WHERE
COMP_ID = 'OAAM';
```

You can skip this pre-upgrade task if you wish to upgrade oaam_offline, oaam_admin, and oaam_server at the same time.

3.5 Installing Oracle Identity and Access Management 11.1.2.2.0

As part of the migration process, you must install Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0).

For information about installing Oracle Identity and Access Management 11.1.2.2.0, see "Installing Oracle Identity and Access Management (11.1.2.2.0)" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

3.6 Creating Oracle Platform Security Services Schema

Create the following schemas by running the Repository Creation utility (RCU) 11.1.2.2.0. IAU (Audit Schema) is optional.

- **Oracle Platform Security Services** (OPSS) - (mandatory)
- **Metadata Services** (MDS) - (mandatory)
- **IAU** (Audit Schema) - (optional)

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

3.7 Upgrading OAAM 10*g* Schema

You must upgrade the OAAM 10*g* schema to 11.1.2.2.0 by running the Upgrade Assistant. To do this, complete the following steps:

1. Run the following command from the location *ORACLE_HOME*/bin to start the Upgrade Assistant:

   On UNIX: `./ua`

   On Windows: `ua.bat`

2. The Oracle Fusion Middleware Upgrade Assistant **Welcome** screen is displayed. Click **Next**.

3. The **Specify Operation** screen is displayed. Select the **Upgrade Oracle Adaptive Access Manager Schema**, and click **Next**.

4. The **Prerequisites** screen is displayed. Select **Database Schema backup completed** and **Database version is certified by Oracle for Fusion Middleware upgrade**, and click **Next**.

   > **Note:** Ensure that you have backed up database schemas before selecting **Database Schema backup completed** on the Prerequisites screen. Also, ensure that the database that you are using is supported for Oracle Adaptive Access Manager 11.1.2.2.0, before selecting the **Database version is certified by Oracle for Fusion Middleware upgrade** on the **Prerequisites** screen.

5. The **Specify OAAM Source Database** screen is displayed. Enter the following information:

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

     `host:port:sid`

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

   Click **Next**.

6. The **Examining Components** screen is displayed.

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

   The **Status** column displays **succeeded** if the action is successful. If the **Status** displays **failed**, check the log file `ua.log` for details. To view the log files, click the link at the bottom of the screen.

   Click **Next**. if the **Status** shows **succeeded**.

7. The **Upgrade Summary** screen is displayed. Click **Upgrade**.

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

   - Status of the upgrade

- Any errors or problems that occur during the upgrade

Click **Next**.

9. The **Upgrade Complete** screen is displayed. This screen confirms that the upgrade was complete.
10. Click **Close**.

3.8 Configuring OAAM 11.1.2.2.0 in a New or Existing Oracle WebLogic Domain

After you install the software, you must configure Oracle Adaptive Access Manager 11.1.2.2.0. You can configure OAAM either in a new or in an existing domain. For more information, see "Configuring Oracle Adaptive Access Manager" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

Note: Ensure that you specify the Oracle Adaptive Access Manager 10*g* database details in the screen where it prompts you to enter the Oracle Adaptive Access Manager 11*g* database details. You must enter the 10*g* credentials because there is no separate 11*g* database. It checks the database for a few system tables, which are not present in Oracle Adaptive Access Manager 10*g* database.

3.9 Configuring Database Security Store

After you configure OAAM 11.1.2.2.0 in a domain, you must run the `configuresecuritystore.py` script to configure the Database Security Store. For more information, see "Configuring Database Security Store for an Oracle Identity and Access Management Domain" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

Note: If you have already run the `configuresecuritystore.py` script as part of the OAAM 11.1.2.2.0 configuration in Section 3.8, "Configuring OAAM 11.1.2.2.0 in a New or Existing Oracle WebLogic Domain", ignore this task.

3.10 Configuring Node Manager

If you wish to start and stop the Managed Servers through the WebLogic Administration console, you must configure the Node Manager, and start it. For information about configuring Node Manager, see "Configuring Node Manager to Start Managed Servers" in the *Oracle Fusion Middleware Administrator's Guide*.

3.11 Starting WebLogic Administration Server

To start the WebLogic Administration Server, follow the instructions described in Appendix A.2.1, "Starting the WebLogic Administration Server".

3.12 Stopping OAAM Managed Servers

If you have started the OAAM Admin Server, OAAM Offline Server (if present), and OAAM Server, you must stop all of them before you can upgrade the OAAM middle tier.

For more information about stopping Managed Server(s), see Appendix A.1.1, "Stopping the Managed Server(s)".

Note: If you have more than one OAAM Server, you must stop all of them.

3.13 Upgrading OAAM Middle Tier Using Upgrade Assistant

You must upgrade the OAAM 10*g* middle tier using Upgrade Assistant. To do this, complete the following steps:

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

      host:*port*/em

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

      The OAAM domain page is displayed.

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

      The **Credentials** page is displayed.

   d. Expand **oaam** and delete the entries related to symmetric keys.
2. Launch Upgrade Assistant by doing the following:

   On UNIX:

   a. Move from your present working directory to the *MW_HOME*/*IAM_HOME*/bin directory using the following command:

      cd *MW_HOME*/*IAM_HOME*/bin

   b. Run the following command:

      ./ua

   On Windows:

   a. Move from your present working directory to the *MW_HOME**IAM_HOME*\bin directory using the following command on the command line:

      cd *MW_HOME**IAM_HOME*\bin

   b. Run the following command:

      ua.bat

   The Oracle Fusion Middleware Upgrade Assistant **Welcome** screen is displayed.
3. Click **Next**.

   The **Specify Operation** screen is displayed.

4. Select **Upgrade Oracle Adaptive Access Manager Middle Tier**.

   The options available in Upgrade Assistant are specific to the Oracle home from which it started. When you start Upgrade Assistant from an Oracle Application Server Identity Management Oracle home, the options shown on the Specify Operation screen are the valid options for an Oracle Application Server Identity Management Oracle home.

5. Click **Next**.

   The **Specify Source Details** screen is displayed.

6. Enter the following information:

   - Click **Browse** and enter the directory location for Oracle Adaptive Access Manager Adaptive Strong Authenticator Web Application 10*g* (ASA) and Adaptive Risk Manager Web Application 10*g* (ARM) applications.
   - **Database Type**: Select the database type from the drop-down list.
   - **Connect String**: Enter the name of the server where your database is running. Use one of the following formats for Oracle Database:

     `//`*`host`*`:`*`port`*`/service` or *`host`*`:`*`port`*`:`*`sid`*

   - **Schema User Name**: Enter the user name for the OAAM schema.
   - **Schema Password**: Enter the password for the OAAM schema.

7. Click **Next**.

   The **Specify WebLogic Server** screen is displayed.

8. Enter the following information about your Oracle WebLogic Server domain:

   - **Host**: The host name of the machine where WebLogic Administration Server is running.
   - **Port**: The listening port of the Administration Server. The default Administration Server port is `7001`.
   - **Username**: The user name that is used to log in to the Administration Server. This is the same username you use to log in to the Administration Console for the domain.
   - **Password**: The password for the administrator account that is used to log in to the Administration Server. This is the same password you use to log in to the Administration Console for the domain.
   - Click **Next**.

   The **Specify Upgrade Options** screen is displayed.

9. Select **Start destination components after successful upgrade**, and click **Next**.

   The **Examining Components** screen is displayed.

   Note: Ensure that Node Manager is running, before you select **Start destination components after successful upgrade**.

10. Click **Next**.

    The **Upgrade Summary** screen is displayed.

11. Click **Upgrade**.

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

- The status of the upgrade
- Any errors or problems that occur during the upgrade

12. Click **Next**.

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

13. Click **Close**.

3.14 Starting OAAM Managed Servers

After you upgrade the OAAM middle tier, you must start the OAAM Managed Servers in the following order:

1. OAAM Admin Server
2. OAAM Offline Server, if you have configured OAAM Offline Server
3. OAAM Server

For more information about starting Managed Server(s), see Appendix A.2.2, "Starting the Managed Server(s)".

> **Note:** Make sure that the OAAM Admin Server is running before you start the OAAM Server.

3.15 Verifying the Migration

To verify if the OAAM 10*g* migration was successful, do the following:

1. Log in to the administration console of Oracle Adaptive Access Manager 11.1.2.2.0, using the administration server username and password, and verify whether the OAAM 10*g* artifacts are migrated to OAAM 11*g*. Use the following URL to log in to the OAAM Admin Server:

   `http://host:port/oaam_admin`

   where

   `host` is the machine on which OAAM Admin Server is running

   `port` is the port number of the OAAM Admin Server

2. Create a user, and assign the `Investigator` role. Log in to the OAAM Admin Server with this user, and verify that you see the Investigator UI successfully.

   For more information about creating OAAM users, see "Creating OAAM Users" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*.

4

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 (11.1.2.2.0).

This chapter contains the following sections:

4.1 Migration Overview

The process of migrating Oracle Single Sign-On 10*g* to Access Manager 11.1.2.2.0 involves installing Oracle Identity and Access Management 11.1.2.2.0, configuring Oracle Access Management Access Manager 11.1.2.2.0, and upgrading the Access Manager middle tier. Oracle Single Sign-On 10*g* to Access Manager 11.1.2.2.0 migration has three scenarios:

- Oracle Delegated Administration Services required after migrating Oracle Single Sign-On 10*g* to Access Manager 11.1.2.2.0

- Oracle Delegated Administration Services required, but Oracle Single Sign-On admin not required after migrating Oracle Single Sign-On 10*g* to Access Manager 11.1.2.2.0
- Oracle Delegated Administration Services not required after migrating Oracle Single Sign-On 10*g* to 11.1.2.2.0

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 1.2, "Migration and Coexistence Scenarios".

4.2 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

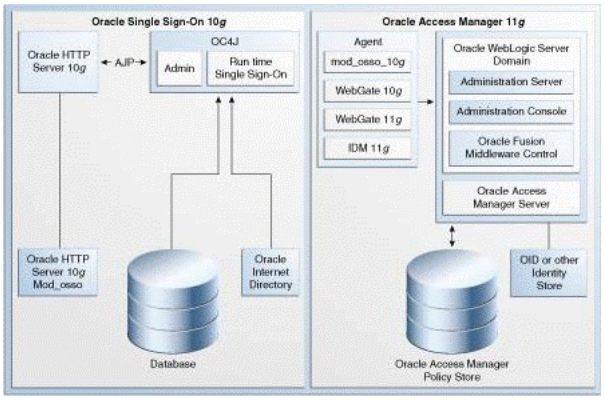
The following components are not migrated to Access Manager 11.1.2.2.0 environment when you run Upgrade Assistant to migrate from Oracle Single Sign-On 10*g*:

- 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.

4.3 Topology Comparison

Figure 4–1 compares a typical Oracle Single Sign-On topology in Oracle Application Server 10*g* with an Access Manager 11.1.2.2.0 topology in Oracle Fusion Middleware 11*g*.

Figure 4–1 Comparison of Typical Oracle Single Sign-On Topologies in Oracle Application Server 10g and Oracle Fusion Middleware 11g



4.4 Migration Scenarios

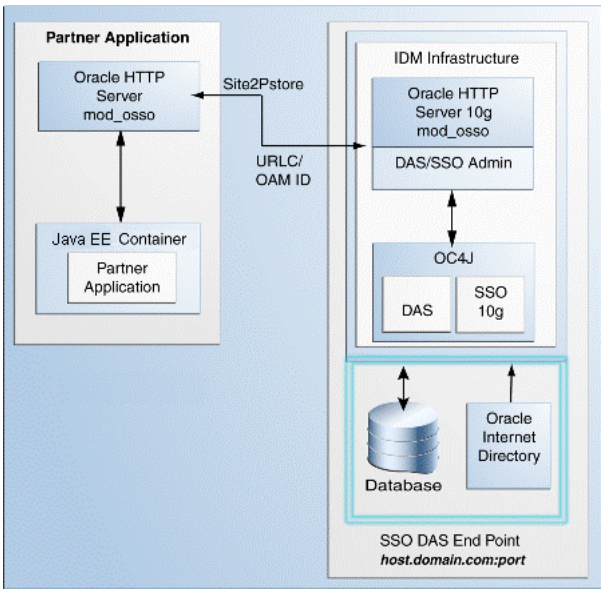
Before you migrate Oracle Single Sign-On 10*g* to Access Manager 11.1.2.2.0, you must consider your Oracle Single Sign-On 10*g* infrastructure (Figure 4–2) and depending on the functionality you choose to retain, you must select one of the following scenarios:

- Oracle Delegated Administration Services Required After Migrating Oracle Single Sign-On 10g to Access Manager 11.1.2.2.0
- Oracle Delegated Administration Services Required, but Oracle Single Sign-On Admin Not Required After Migrating Oracle Single Sign-On to Access Manager 11.1.2.2.0
- Oracle Delegated Administration Services Not Required After Migrating Oracle Single Sign-On to Access Manager 11.1.2.2.0

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

Figure 4–2 illustrates the Oracle Single Sign-On 10*g* topology.

Figure 4–2 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.

4.4.1 Oracle Delegated Administration Services Required After Migrating Oracle Single Sign-On 10*g* to Access Manager 11.1.2.2.0

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 11.1.2.2.0. Figure 4–3 illustrates the scenario.

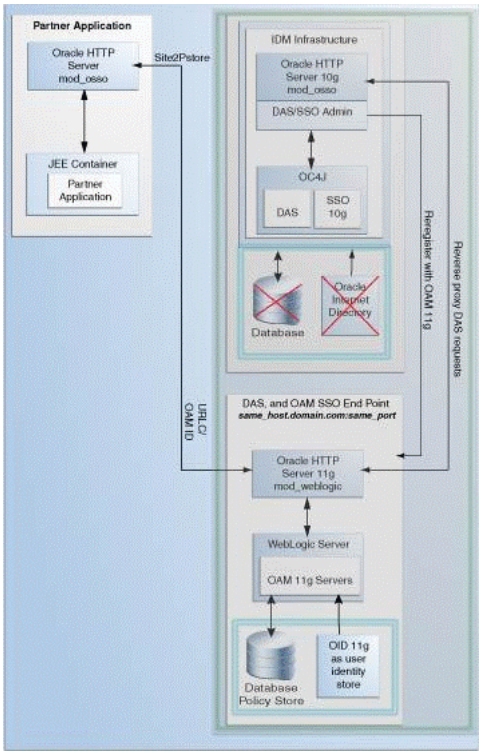
Note the following points when using this migration scenario:

- 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 11.1.2.2.0. Therefore, the Oracle Single Sign-On 10*g* server is no longer accessed. Instead, partner applications use Access Manager 11.1.2.2.0.
- 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 11.1.2.2.0 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 4–3 Oracle Delegated Administration Services Required After Migrating from Oracle Single Sign-On



To use this migration scenario, follow the steps listed in Table 4–1.

4.4.2 Oracle Delegated Administration Services Required, but Oracle Single Sign-On Admin Not Required After Migrating Oracle Single Sign-On to Access Manager 11.1.2.2.0

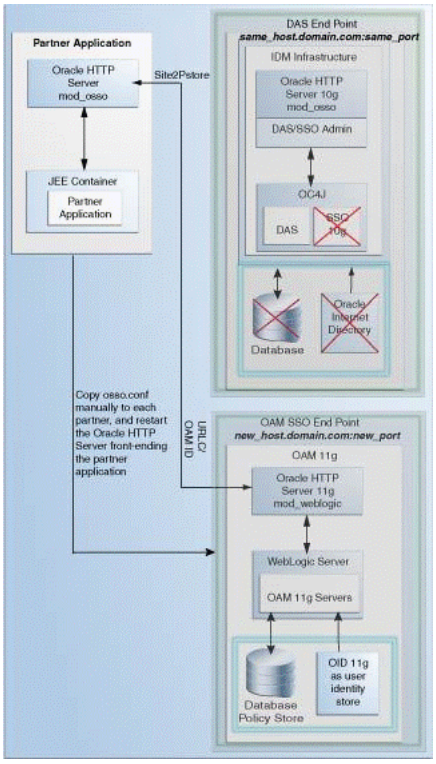
Use this migration scenario if you do not require the Oracle Single Sign-On Admin tool application, but you require the Oracle Delegated Administration Services application after migrating from Oracle Single Sign-On 10*g* to Access Manager 11.1.2.2.0. Figure 4–4 illustrates the scenario.

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 11.1.2.2.0 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 11.1.2.2.0 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 4–4 Oracle Single Sign-On Administration Server Not required



To use this migration scenario, follow the steps listed in Table 4–1.

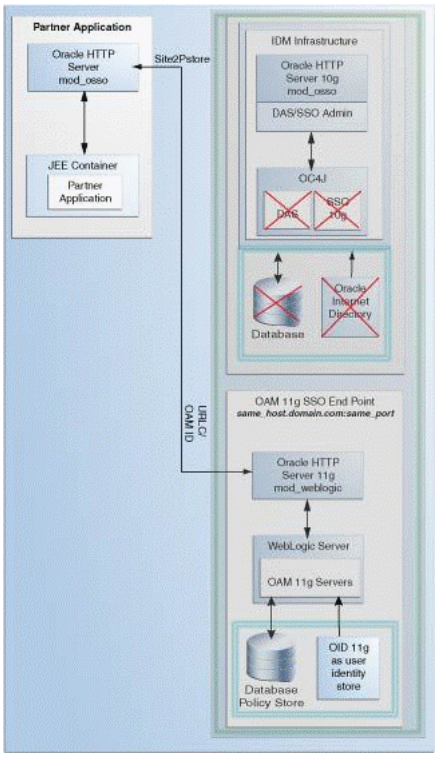
4.4.3 Oracle Delegated Administration Services Not Required After Migrating Oracle Single Sign-On to Access Manager 11.1.2.2.0

Use this migration scenario if you do not require the Oracle Delegated Administration Services application or the Oracle Single Sign-On Admin tool. Figure 4–5 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 11.1.2.2.0. 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 4–5 Oracle Delegated Administration Services Not Required



To use this migration scenario, follow the steps listed in Table 4–1.

4.5 Migration Roadmap

Table 4–1 describes the tasks that should be completed for each of the Oracle Single Sign-On 10*g* migration scenarios.

Table 4–1 Migration Scenarios and Tasks

Scenario	Tasks to be Completed
Oracle Delegated Administration Services Required After Migrating Oracle Single Sign-On 10g to Access Manager 11.1.2.2.0	▪ Section 4.6, "Prerequisites for Migration" ▪ Section 4.7, "Understanding the Access Manager 11.1.2.2.0 Topology" ▪ Section 4.8, "Optional: Upgrading the Oracle Database" ▪ Section 4.9, "Creating Schemas Using Repository Creation Utility" ▪ Section 4.10.1, "Installing and Configuring Access Manager 11.1.2.2.0 Using Oracle Single Sign-On 10g Host Name and Port Number" ▪ Section 4.11, "Upgrading Access Manager 11.1.2.2.0 Middle Tier Using Upgrade Assistant" ▪ Section 4.12, "Performing Post-Migration Tasks" ▪ Section 4.13, "Verifying the Migration"

Table 4–1 (Cont.) Migration Scenarios and Tasks

Scenario	Tasks to be Completed
Oracle Delegated Administration Services Required, but Oracle Single Sign-On Admin Not Required After Migrating Oracle Single Sign-On to Access Manager 11.1.2.2.0	■ Section 4.6, "Prerequisites for Migration" ■ Section 4.7, "Understanding the Access Manager 11.1.2.2.0 Topology" ■ Section 4.8, "Optional: Upgrading the Oracle Database" ■ Section 4.9, "Creating Schemas Using Repository Creation Utility" ■ Section 4.10.2, "Installing and Configuring Access Manager 11.1.2.2.0 Using New Host Name or New Port Number" ■ Section 4.11, "Upgrading Access Manager 11.1.2.2.0 Middle Tier Using Upgrade Assistant" ■ Section 4.12, "Performing Post-Migration Tasks" ■ Section 4.13, "Verifying the Migration"
Oracle Delegated Administration Services Not Required After Migrating Oracle Single Sign-On to Access Manager 11.1.2.2.0	■ Section 4.6, "Prerequisites for Migration" ■ Section 4.7, "Understanding the Access Manager 11.1.2.2.0 Topology" ■ Section 4.8, "Optional: Upgrading the Oracle Database" ■ Section 4.9, "Creating Schemas Using Repository Creation Utility" ■ Section 4.10.1, "Installing and Configuring Access Manager 11.1.2.2.0 Using Oracle Single Sign-On 10g Host Name and Port Number" ■ Section 4.11, "Upgrading Access Manager 11.1.2.2.0 Middle Tier Using Upgrade Assistant" ■ Section 4.12, "Performing Post-Migration Tasks" ■ Section 4.13, "Verifying the Migration"

4.6 Prerequisites for Migration

You must complete the following prerequisites for migrating Oracle Single Sign-On 10*g* to Access Manager 11.1.2.2.0:

1. Read the system requirements and certification documents to ensure that your environment meets the minimum requirements for the products you are installing.

   ■ *Oracle Fusion Middleware System Requirements and Specifications*

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

   ■ *Oracle Fusion Middleware Supported System Configurations*

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

   ■ For interoperability and compatibility issues that may arise when installing, refer to *Oracle Fusion Middleware Interoperability and Compatibility Guide*.

   This document contains important information regarding the ability of Oracle Fusion Middleware products to function with previous versions of other Oracle Fusion Middleware, Oracle, or third-party products. This information

is applicable to both new Oracle Fusion Middleware users and existing users who are upgrading their existing environment.

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 1.4, "Supported Starting Points for Migration and Coexistence".

4.7 Understanding the Access Manager 11.1.2.2.0 Topology

Before you begin the migration process, get familiar with the topology of Access Manager 11.1.2.2.0.

For more information, see Section 4.3, "Topology Comparison".

4.8 Optional: Upgrading the Oracle Database

When you are migrating an Oracle Single Sign-On environment to Access Manager 11.1.2.2.0, 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.

4.9 Creating Schemas Using Repository Creation Utility

You must create the necessary schemas in the database in order to configure Access Manager 11.1.2.2.0. 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 11.1.2.2.0, 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*.:

4.10 Installing and Configuring the Access Manager 11.1.2.2.0 Middle Tier

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

- Installing and Configuring Access Manager 11.1.2.2.0 Using Oracle Single Sign-On 10g Host Name and Port Number
- Installing and Configuring Access Manager 11.1.2.2.0 Using New Host Name or New Port Number

4.10.1 Installing and Configuring Access Manager 11.1.2.2.0 Using Oracle Single Sign-On 10*g* Host Name and Port Number

Table 4–2 lists the steps to install and configure the Access Manager 11.1.2.2.0 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 11.1.2.2.0.

Table 4–2 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 11.1.2.2.0	See, "Installing Oracle Identity and Access Management (11.1.2.2.0)" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.
5	Configuring Oracle Access Management Access Manager 11.1.2.2.0.	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 11.1.2.2.0 Managed Server with the Oracle HTTP Server 11g	See, Front-Ending Access Manager 11.1.2.2.0 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 11.1.2.2.0 Managed Server with Oracle HTTP Server 11*g*

You must use `mod_wl_ohs` to front-end Access Manager 11.1.2.2.0 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 11.1.2.2.0 Managed server. To restart the servers, you must first stop them, and then start.

   For information about stopping the Administration Server and Managed Server(s), see Appendix A.1, "Stopping the Servers".

   For information about starting the Administration Server and Managed Server(s), Appendix A.2, "Starting the Servers".

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 11.1.2.2.0. To do so, complete the following steps:

1. Log in to the Oracle Access Management 11.1.2.2.0 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
```

4.10.2 Installing and Configuring Access Manager 11.1.2.2.0 Using New Host Name or New Port Number

Table 4–3 lists the steps you must perform when installing and configuring the Access Manager 11.1.2.2.0 middle tier, using a new host name or port number for Oracle Access Manager.

Table 4–3 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 (11.1.2.2.0)	See, "Installing Oracle Identity and Access Management (11.1.2.2.0)" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.
3	Configuring Oracle Access Management Access Manager 11.1.2.2.0	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*.

4.11 Upgrading Access Manager 11.1.2.2.0 Middle Tier Using Upgrade Assistant

When you install Access Manager 11.1.2.2.0, 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 11.1.2.2.0 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 11.1.2.2.0 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**.

4.12 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 11.1.2.2.0:

- Configuring Oracle Portal 10g with Access Manager 11.1.2.2.0 Server if the Oracle HTTP Server Port is Changed
- Configuring Oracle Access Management 11.1.2.2.0 Administration Console to Align Roles
- Copying the osso.conf File
- Configuring Oracle Business Intelligence Discoverer 11g with Access Manager 11.1.2.2.0
- 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 11.1.2.2.0
- Additional Step for Oracle Internet Directory Configured in SSL Server Authentication Mode
- Additional Access Manager Post-Migration Tasks
- Decommissioning Oracle Single Sign-On 10g

4.12.1 Configuring Oracle Portal 10*g* with Access Manager 11.1.2.2.0 Server if the Oracle HTTP Server Port is Changed

After migrating the Oracle Portal's Oracle Single Sign-On Server to the Access Manager 11.1.2.2.0 Server, you must update the Oracle Portal schema with information about the Access Manager 11.1.2.2.0 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 11.1.2.2.0 Managed Server host name and port number.

4.12.2 Configuring Oracle Access Management 11.1.2.2.0 Administration Console to Align Roles

After migration, the Oracle Access Management 11.1.2.2.0 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 11.1.2.2.0 Administrator for the Oracle Access Management 11.1.2.2.0 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 11.1.2.2.0 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")
```

4.12.3 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 11.1.2.2.0.

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.

4.12.4 Configuring Oracle Business Intelligence Discoverer 11*g* with Access Manager 11.1.2.2.0

After migrating the Oracle Business Intelligence Discoverer's Oracle Single Sign-On server to the Access Manager 11.1.2.2.0 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
   ```

4.12.5 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 11.1.2.2.0 console. To do this, complete the following steps:

1. Log in to the Oracle Access Management 11.1.2.2.0 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 11.1.2.2.0 console

- *port* refers to the designated bind port for the Oracle Access Management 11.1.2.2.0 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 4–4 with the right values for **Name**, **Type**, and **Value** fields as specified in the table. Click **Add** after adding each header.

Table 4–4 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 Server(s) by completing the following tasks. To restart the servers, you must stop them first and start again.

    For information about stopping the Administration Server and the Managed Server(s), see Appendix A.1, "Stopping the Servers".

    For information about starting the Administration Server and the Managed Server(s), see Appendix A.2, "Starting the Servers".

4.12.6 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 11.1.2.2.0 console. To do this, complete the following steps:

1. Log in to the Oracle Access Management 11.1.2.2.0 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 11.1.2.2.0 administration console
   - *port* refers to the designated bind port for the Oracle Access Management 11.1.2.2.0 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**.

4.12.7 Setting the Migrated Identity Store as Default Store and System Store for Access Manager 11.1.2.2.0

After you migrate Oracle Single Sign-On 10*g* to Access Manager 11.1.2.2.0, you must explicitly set the `migratedUserIdentityStore` as the Default Store and System Store for Access Manager 11.1.2.2.0. To do this, refer to "Setting the Default Store and System Store" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.

4.12.8 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 11.1.2.2.0 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 11.1.2.2.0 Managed Servers. To restart the servers, you must stop them first and start again.

   For information about stopping the Administration Server and the Managed Server(s), see Appendix A.1, "Stopping the Servers".

   For information about starting the Administration Server and the Managed Server(s), see Appendix A.2, "Starting the Servers".

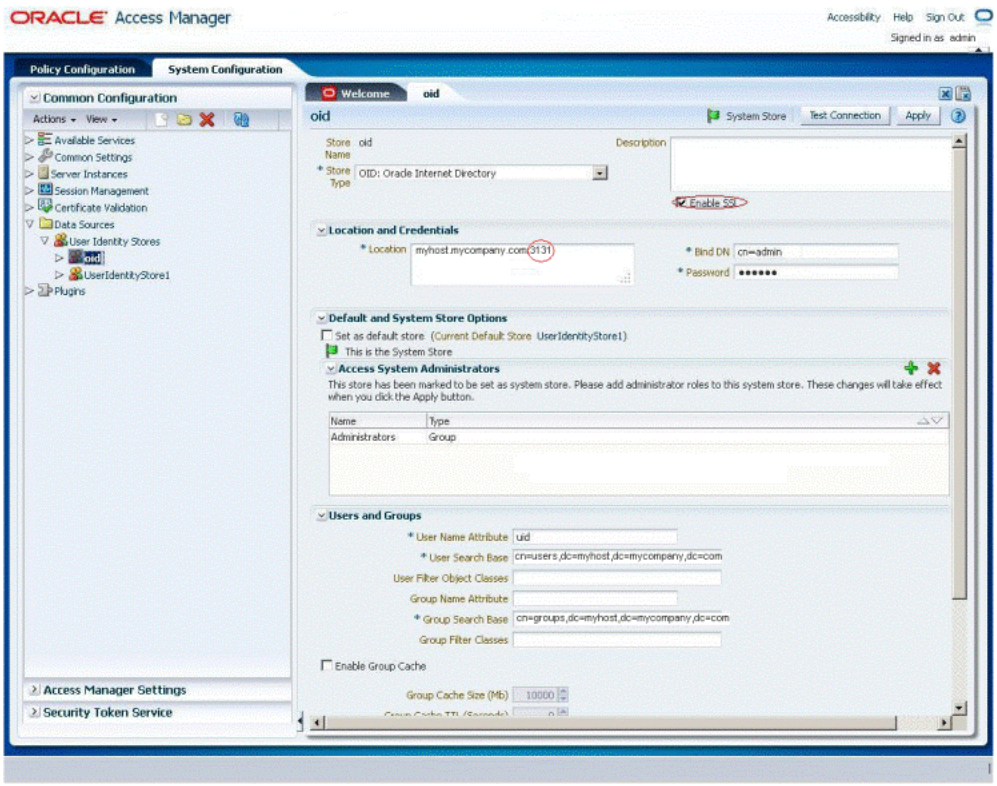
3. Log in to the Oracle Access Management 11.1.2.2.0 console using the following URL:

   ```
   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 4–6 shows the Access Manager console where you create new User Identity Store.

Figure 4–6 Creating New User Identity Store



4.12.9 Additional Access Manager Post-Migration Tasks

You must perform the following additional post-migration tasks after migrating to Access Manager 11.1.2.2.0:

- 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 11.1.2.2.0 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 11.1.2.2.0 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
```

4.12.10 Decommissioning Oracle Single Sign-On 10*g*

After migrating to Access Manager 11.1.2.2.0, 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
```

4.13 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 11.1.2.2.0 Administration Server is up and running, log in to the Oracle Access Management 11.1.2.2.0 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 11.1.2.2.0 administration console.
   - *`port`* refers to the designated bind port for the Oracle Access Management 11.1.2.2.0 console, which is the same as the bind port for the Administration Server.

3. To verify that the Access Manager 11.1.2.2.0 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 11.1.2.2.0 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*.

5

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 (11.1.2.2.0).

The chapter contains the following sections:

5.1 Migration Overview

This section introduces two tools that are used in the process of migrating Sun OpenSSO Enterprise 8.0 to Oracle Access Manager 11.1.2.2.0.

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 11.1.2.2.0, 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 11.1.2.2.0 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 11.1.2.2.0, based on the understanding of the artifacts supported in Access Manager 11.1.2.2.0.

You can generate the assessment report more than once before you can migrate the OpenSSO Enterprise 8.0 to Access Manager 11.1.2.2.0.

Migration Tool

The Migration tool migrates the following artifacts of OpenSSO Enterprise 8.0 to Access Manager 11.1.2.2.0:

- 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 1.2, "Migration and Coexistence Scenarios".

5.2 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

5.2.1 Complete Migration

Complete Migration migrates all compatible agents, policies, user stores, and authentication stores of OpenSSO Enterprise 8.0 to Access Manager 11.1.2.2.0. 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 11.1.2.2.0 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.

5.2.2 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 11.1.2.2.0. 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, user stores and authentication stores will be migrated automatically.

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 migrated 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.

5.2.3 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 11.1.2.2.0. 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 11.1.2.2.0 configuration store is retrieved, is incremented by one, and is saved back to the Access Manager 11.1.2.2.0 configuration store.

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

5.3 Migration Summary

This sections summarizes the artifacts of OpenSSO Enterprise 8.0 that are compatible with Access Manager 11.1.2.2.0. 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

5.3.1 Summary of Migration of Agents

This section summarizes the migration of agents from OpenSSO Enterprise 8.0 to Access Manager 11.1.2.2.0.

- 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 11.1.2.2.0. 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 11.1.2.2.0.
- 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 11.1.2.2.0 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`.

5.3.2 Summary of Migration of Policies

This section summarizes the migration of policies from OpenSSO Enterprise 8.0 to Access Manager 11.1.2.2.0.

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 11.1.2.2.0:

- **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 11.1.2.2.0. All the auto policies can be migrated to Access Manager 11.1.2.2.0.
- **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 11.1.2.2.0. Semi policies are not migrated to Access Manager 11.1.2.2.0.
- **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 11.1.2.2.0. Manual policies are not migrated to Access Manager 11.1.2.2.0.

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 11.1.2.2.0) are not supported in Access Manager 11.1.2.2.0.

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 11.1.2.2.0.

Conditions

- Active Session Time
  - This condition of OpenSSO Enterprise policy is mapped to the attribute `Session Expiry Time` of the AttributeCondition in Access Manager 11.1.2.2.0.
  - The attribute `Terminate session` of this condition is ignored during migration as the appropriate mapping of this attribute does not exist in Access Manager 11.1.2.2.0.
- Authentication by Module Instance
  - This condition of OpenSSO Enterprise policy is migrated to Access Manager 11.1.2.2.0 as `AuthN` scheme, and not as a condition.
  - Table 5–1 lists the authentication modules of OpenSSO Enterprise 8.0 that are migrated and mapped with `AuthN` scheme into Access Manager 11.1.2.2.0.

Table 5–1 Mapping of Authentication Module

Authentication Module in OpenSSO Enterprise 8.0	Authentication Plug-in in Access Manager 11.1.2.2.0
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 11.1.2.2.0 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 11.1.2.2.0.

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 11.1.2.2.0 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 11.1.2.2.0 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 11.1.2.2.0.
  - 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 11.1.2.2.0.
  - 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 11.1.2.2.0.
  - The condition `DNS name` is not supported in Access Manager 11.1.2.2.0.
- LDAP Filter Condition
  - This condition in OpenSSO Enterprise policy is mapped to `Identity condition` in Access Manager 11.1.2.2.0.
  - 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 11.1.2.2.0.
- Time (day, date, time, and time zone)
  - This condition in OpenSSO Enterprise 8.0 policy is mapped to `Time condition` in Access Manager 11.1.2.2.0.
  - 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 11.1.2.2.0 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 11.1.2.2.0. 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 11.1.2.2.0 with the type Http header.

5.3.3 Summary of Migration of User Stores

This section summarizes the migration of user stores from OpenSSO Enterprise 8.0 to Access Manager 11.1.2.2.0.

OpenSSO Enterprise has three types of user stores:

- **Active Directory**: This user store can be migrated to Access Manager 11.1.2.2.0.
- **Generic LDAPv3**: This user store can be migrated to Access Manager 11.1.2.2.0.
- **Sun DS with OpenSSO schema**: This user store cannot be migrated to Access Manager 11.1.2.2.0, as no supported data store type is available in 11.1.2.2.0.

5.3.4 Summary of Migration of Authentication Stores

This section summarizes the migration of authentication stores from OpenSSO Enterprise 8.0 to Access Manager 11.1.2.2.0.

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 11.1.2.2.0:

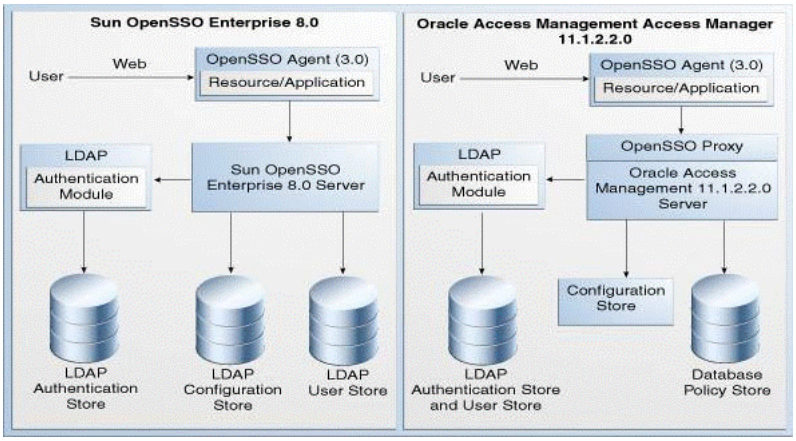
- LDAP in OpenSSO Enterprise 8.0 is mapped to OAM LDAP in Access Manager 11.1.2.2.0.
- Certificate in OpenSSO Enterprise 8.0 is mapped to X509 in Access Manager 11.1.2.2.0.
- Windows Desktop SSO in OpenSSO Enterprise 8.0 is mapped to Kerberos Access Manager 11.1.2.2.0.

All authentication stores with type LDAP are migrated to Access Manager 11.1.2.2.0 with name `AS_RealmName_Modulename`. The authentication stores with type other than LDAP are not migrated.

5.4 Topology Comparison

Figure 5–1 compares the topologies of Sun OpenSSO Enterprise 8.0 and Access Manager 11.1.2.2.0.

Figure 5–1 OpenSSO Enterprise 8.0 and Access Manager 11.1.2.2.0 Topologies



5.5 Migration Roadmap

Table 5–2 lists the steps to migrate Sun OpenSSO Enterprise 8.0 to Access Manager 11.1.2.2.0.

Table 5–2 Task Roadmap

Task No	Task	For More Information
1	Complete the prerequisites.	See, Prerequisites for Migration
2	Install Oracle Identity and Access Management 11.1.2.2.0.	See, Installing Oracle Identity and Access Management 11.1.2.2.0
3	Configure Oracle Access Management Access Manager 11.1.2.2.0.	See, Configuring Oracle Access Management Access Manager 11.1.2.2.0
4	Generate the assessment report, and analyze what artifacts can be migrated to Access Manager 11.1.2.2.0. 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 11.1.2.2.0 by running the migration tool.	See, Migrating the Artifacts of OpenSSO Enterprise 8.0 to Access Manager 11.1.2.2.0

Table 5–2 (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

5.6 Prerequisites for Migration

You must complete the following prerequisites for migrating OpenSSO Enterprise 8.0 to Access Manager 11.1.2.2.0:

1. Read the system requirements and certification documents to ensure that your environment meets the minimum requirements for the products you are installing.

   - *Oracle Fusion Middleware System Requirements and Specifications*

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

   - *Oracle Fusion Middleware Supported System Configurations*

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

   - For interoperability and compatibility issues that may arise when installing, refer to *Oracle Fusion Middleware Interoperability and Compatibility Guide*.

     This document contains important information regarding the ability of Oracle Fusion Middleware products to function with previous versions of other Oracle Fusion Middleware, Oracle, or third-party products. This information is applicable to both new Oracle Fusion Middleware users and existing users who are upgrading their existing environment.

     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 1.4, "Supported Starting Points for Migration and Coexistence".

5.7 Installing Oracle Identity and Access Management 11.1.2.2.0

As part of migration process, you must freshly install Oracle Identity and Access Management 11.1.2.2.0. This 11.1.2.2.0 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 11.1.2.2.0, see "Installing Oracle Identity and Access Management (11.1.2.2.0)" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

5.8 Configuring Oracle Access Management Access Manager 11.1.2.2.0

Configure Access Manager 11.1.2.2.0, and create a domain.

For information about configuring Access Manager 11.1.2.2.0, see "Configuring Oracle Access Management" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

5.9 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 11.1.2.2.0.

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.

5.9.1 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.

5.9.2 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.

5.9.3 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 5.9.1, "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
```

5.9.4 Analyzing the Assessment Report

The OpenSSO Agent assessment tool generates five Comma Separated Values (CSV) 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 11.1.2.2.0.

Table 5–3 lists the CSV files that are generated when you run the OpenSSO Agent assessment tool.

Table 5–3 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 11.1.2.2.0.
`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.

5.10 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.

5.11 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 above values are case-insensitive.

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 5.12, "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 11.1.2.2.0.

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 5.12, "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 11.1.2.2.0, which in turn is a complete migration.

5.12 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 5–4 describes the values you must specify for each of the properties in the properties file.

Table 5–4 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.
`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.

Table 5–4 (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 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.

Table 5–4 (Cont.) Property File Values

Property	Description
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.

5.13 Migrating the Artifacts of OpenSSO Enterprise 8.0 to Access Manager 11.1.2.2.0

Before you start the actual migration of the artifacts from OpenSSO Enterprise 8.0 to Access Manager 11.1.2.2.0, make sure that you have generated the assessment report (as described in Section 5.9, "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 11.1.2.2.0, do the following:

1. If you wish to perform Incremental Migration, make sure you have completed the additional steps as described in Section 5.11, "Additional Steps for Incremental Migration".
2. Make sure you have created the properties file as described in Section 5.12, "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 11.1.2.2.0:

   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/def*/oam_migration.properties"

   On Windows:
   oamMigrate(oamMigrateType="OpenSSO",pathMigrationPropertiesFile="*abc**def*\\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 5.2, "Modes of Migration".

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

5.14 Performing Post-Migration Tasks

After you migrate OpenSSO Enterprise 8.0 to Access Manager 11.1.2.2.0, 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.appserver.v81.AmASAgentServiceResolver
      ```

      For WebLogic agent, set the following property:

      ```
      com.sun.identity.agents.config.service.resolver=com.sun.identity.agents.weblogic.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 11.1.2.2.0. 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 11.1.2.2.0 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 11.1.2.2.0 console. To do this, complete the following steps:

a. Log in to the Oracle Access Management 11.1.2.2.0 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**.

4. Restart the Access Manager Managed Server(s) and the web container instances for the agents that you migrated, by completing the following steps:

a. Stop the web container instance for the migrated agent.

b. Stop the Access Manager Managed Server(s).

For information about stopping the Managed Server(s), see Appendix A.1.1, "Stopping the Managed Server(s)".

c. Start the Access Manager Managed Server(s).

For information about starting the Managed Server(s), see Appendix A.2.2, "Starting the Managed Server(s)".

d. Start the web container instance for the migrated agent.

5.15 Verifying the Migration

To verify the migration, do the following:

1. Log in to the Oracle Access Management 11.1.2.2.0 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 11.1.2.2.0 console.
- *port* refers to the designated bind port for the Oracle Access Management 11.1.2.2.0 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 11.1.2.2.0.

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.

6

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 (11.1.2.2.0).

The chapter contains the following sections:

6.1 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 11.1.2.2.0.

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 11.1.2.2.0, 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 11.1.2.2.0 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 11.1.2.2.0 and what cannot be migrated to Access Manager 11.1.2.2.0 based on the understanding of the supported artifacts in Access Manager 11.1.2.2.0.

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 11.1.2.2.0:

- 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 1.2, "Migration and Coexistence Scenarios".

6.2 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

6.2.1 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 11.1.2.2.0. 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 11.1.2.2.0 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.

6.2.2 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 11.1.2.2.0. 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.

6.2.3 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 11.1.2.2.0. 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 11.1.2.2.0 configuration store is retrieved, is incremented by one, and is saved back to Access Manager 11.1.2.2.0 configuration store.

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

6.3 Migration Summary

This sections summarizes the artifacts of Sun Java System Access Manager 7.1 that are compatible with Access Manager 11.1.2.2.0. 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

6.3.1 Summary of Migration of Agents

This section summarizes the migration of agents from Sun Java System Access Manager 7.1 to Access Manager 11.1.2.2.0.

- 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 11.1.2.2.0 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`.

6.3.2 Summary of Migration of Policies

This section summarizes the migration of policies from Sun Java System Access Manager 7.1 to Access Manager 11.1.2.2.0.

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 11.1.2.2.0:

- **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 11.1.2.2.0. All the auto policies can be migrated to Access Manager 11.1.2.2.0.
- **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 11.1.2.2.0. Semi policies are not migrated to Access Manager 11.1.2.2.0.
- **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 11.1.2.2.0. Manual policies are not migrated to Access Manager 11.1.2.2.0.

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 11.1.2.2.0) are not supported in Access Manager 11.1.2.2.0.

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 11.1.2.2.0.

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 11.1.2.2.0.
  - The attribute `Terminate session` of this condition is ignored during migration as the appropriate mapping of this attribute does not exist in Access Manager 11.1.2.2.0.
- Authentication by Module Instance
  - This condition of Sun Java System Access Manager 7.1 policy is migrated to Access Manager 11.1.2.2.0 as `AuthN` scheme, and not as a condition.
  - Table 6–1 lists the authentication modules of Sun Java System Access Manager 7.1 that are migrated and mapped with the `AuthN` scheme into Access Manager 11.1.2.2.0.

Table 6–1 Mapping of Authentication Module

Authentication Module in Sun Java System Access Manager 7.1	Authentication Plug-in in Access Manager 11.1.2.2.0
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 11.1.2.2.0 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 11.1.2.2.0.

    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 11.1.2.2.0 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 11.1.2.2.0 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 11.1.2.2.0.
  - 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 11.1.2.2.0.
  - 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 11.1.2.2.0.
  - The condition `DNS name` is not supported in Access Manager 11.1.2.2.0.
- LDAP Filter Condition
  - This condition in Sun Java System Access Manager 7.1 policy is mapped to `Identity condition` in Access Manager 11.1.2.2.0.
  - 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 11.1.2.2.0.
- 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 11.1.2.2.0.
  - 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 11.1.2.2.0 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 11.1.2.2.0. 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 11.1.2.2.0 with the type Http header.

6.3.3 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 11.1.2.2.0.

OpenSSO Enterprise has three types of user stores:

- **Active Directory**: This user store can be migrated to Access Manager 11.1.2.2.0.
- **Generic LDAPv3**: This user store can be migrated to Access Manager 11.1.2.2.0.
- **Sun DS with OpenSSO schema**: This user store cannot be migrated to Access Manager 11.1.2.2.0, as no supported data store type is available in 11.1.2.2.0.

6.3.4 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 11.1.2.2.0.

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 11.1.2.2.0:

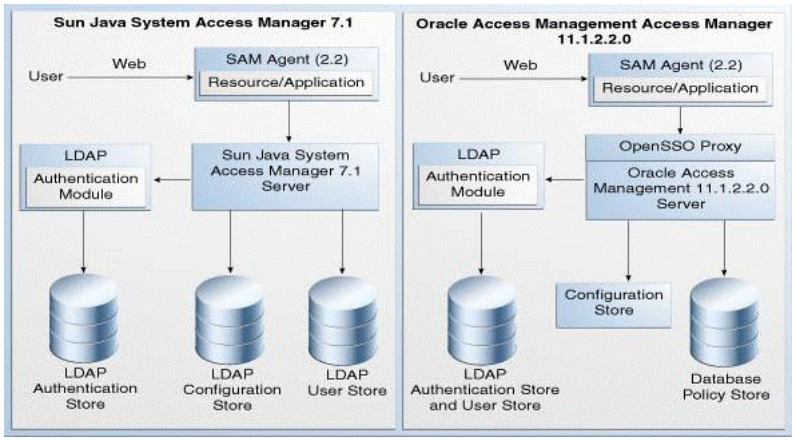
- LDAP in Sun Java System Access Manager 7.1 is mapped to OAM LDAP in Access Manager 11.1.2.2.0.
- Certificate in Sun Java System Access Manager 7.1 is mapped to X509 in Access Manager 11.1.2.2.0.
- Windows Desktop SSO in Sun Java System Access Manager 7.1 is mapped to Kerberos Access Manager 11.1.2.2.0.

All authentication stores with type LDAP are migrated to Access Manager 11.1.2.2.0 with name `AS_RealmName_Modulename`. The authentication stores with type other than LDAP are not migrated.

6.4 Topology Comparison

Figure 6–1 compares the topologies of Sun Java System Access Manager 7.1 and Access Manager 11.1.2.2.0.

Figure 6–1 Sun Java System Access Manager 7.1 and Access Manager 11.1.2.2.0 Topologies



6.5 Migration Roadmap

Table 6–2 lists the steps to migrate Sun Java System Access Manager 7.1 to Access Manager 11.1.2.2.0.

Table 6–2 Task Roadmap

Task No	Task	For More Information
1	Complete the prerequisites.	See, Prerequisites for Migration
2	Install Oracle Identity and Access Management 11.1.2.2.0.	See, Installing Oracle Identity and Access Management 11.1.2.2.0
3	Configure Oracle Access Management Access Manager 11.1.2.2.0.	See, Configuring Oracle Access Manager 11.1.2.2.0
4	Generate the assessment report, and analyze what artifacts can be migrated to Access Manager 11.1.2.2.0. 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 11.1.2.2.0 by running the migration tool.	See, Migrating the Artifacts of Sun Java System Access Manager 7.1 to OAM 11.1.2.2.0
9	Complete the post-migration steps.	See, Performing Post-Migration Tasks
10	Verify the migration.	See, Verifying the Migration

6.6 Prerequisites for Migration

You must complete the following prerequisites for migrating Sun Java System Access Manager 7.1 to Access Manager 11.1.2.2.0:

1. Read the system requirements and certification documents to ensure that your environment meets the minimum requirements for the products you are installing.
   - *Oracle Fusion Middleware System Requirements and Specifications*

     This document contains information related to hardware and software requirements, minimum disk space and memory requirements, and required system libraries, packages, or patches.
   - *Oracle Fusion Middleware Supported System Configurations*

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

- For interoperability and compatibility issues that may arise when installing, refer to *Oracle Fusion Middleware Interoperability and Compatibility Guide*.

  This document contains important information regarding the ability of Oracle Fusion Middleware products to function with previous versions of other Oracle Fusion Middleware, Oracle, or third-party products. This information is applicable to both new Oracle Fusion Middleware users and existing users who are upgrading their existing environment.

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 1.4, "Supported Starting Points for Migration and Coexistence".

6.7 Installing Oracle Identity and Access Management 11.1.2.2.0

As part of the migration process, you must freshly install Oracle Identity and Access Management 11.1.2.2.0 This 11.1.2.2.0 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 11.1.2.2.0, see "Installing Oracle Identity and Access Management (11.1.2.2.0)" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

6.8 Configuring Oracle Access Manager 11.1.2.2.0

After you install Oracle Identity and Access Management 11.1.2.2.0, you must configure Access Manager 11.1.2.2.0 in a domain.

For more information about configuring Access Manager 11.1.2.2.0, see "Configuring Oracle Access Management" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

6.9 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 11.1.2.2.0.

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.

6.9.1 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.

6.9.2 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.

6.9.3 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`

   Note: The above keys and values are case-sensitive.

   Click **Add** after typing each attribute.
6. Click **Save**.

6.9.4 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 6.9.1, "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
```

6.9.5 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 11.1.2.2.0.

Table 6–3 lists the CSV files that are generated when you run the assessment tool.

Table 6–3 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 11.1.2.2.0.
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.

6.10 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.

6.11 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 above values are case-insensitive.

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 6.12, "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 11.1.2.2.0.

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 6.12, "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 11.1.2.2.0, which in turn is a complete migration.

6.12 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 6–4 describes the values you must specify for each of the properties in the properties file.

Table 6–4 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 6–4 (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 6–4 (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 openSSOSMIncludeFilePathproperties 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.

6.13 Migrating the Artifacts of Sun Java System Access Manager 7.1 to OAM 11.1.2.2.0

Before you start the actual migration of the artifacts from Sun Java System Access Manager 7.1 to Access Manager 11.1.2.2.0, make sure that you have generated the assessment report (as described in Section 6.9, "Generating the Assessment Report"), and analyzed what artifacts can be migrated to Access Manager 11.1.2.2.0.

To migrate Sun Java System Access Manager 7.1 to Access Manager 11.1.2.2.0, do the following:

1. If you wish to perform Incremental Migration, make sure you have completed the additional steps as described in Section 6.11, "Additional Steps for Incremental Migration".
2. Make sure you have created the properties file as described in Section 6.12, "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 11.1.2.2.0:

```
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 6.2, "Modes of Migration".

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

6.14 Performing Post-Migration Tasks

After you migrate Sun Java System Access Manager 7.1 to Access Manager 11.1.2.2.0, 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 11.1.2.2.0 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 11.1.2.2.0. 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 11.1.2.2.0 console using the following URL:

      `http://host:port/oamconsole`

where *host* is the machine on which Access Manager 11.1.2.2.0 is running, and *port* is the port number.

b. Go to the **Launch Pad** tab.

c. Click on **User Identity Stores** under the section **Configuration**. 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 11.1.2.2.0 console. To do this, complete the following steps:

   a. Log in to the Oracle Access Management 11.1.2.2.0 console using the URL:

      `http://host:port/oamconsole`

   b. Go to the **Launch Pad** tab.

   c. Click on **User Identity Stores** under the section **Configuration**.

   d. Select the authentication store to be edited.

   e. 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.

   f. Click **Apply**.

5. Restart the Access Manager Managed Server(s) and the web container instances for the agents that you migrated, by completing the following steps:

   a. Stop the web container instance for the migrated agent.

   b. Stop the Access Manager Managed Server(s).

      For information about stopping the Managed Server(s), see Appendix A.1.1, "Stopping the Managed Server(s)".

   c. Start the Access Manager Managed Server(s).

      For information about starting the Managed Server(s), see Appendix A.2.2, "Starting the Managed Server(s)".

   d. Start the web container instance for the migrated agent.

6.15 Verifying the Migration

To verify the migration, do the following:

1. Log in to the Oracle Access Management 11.1.2.2.0 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 11.1.2.2.0 console.
   - *port* refers to the designated bind port for the Oracle Access Management 11.1.2.2.0 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 11.1.2.2.0.

2. Access any protected page using the URL. The URL now redirects you to the Oracle Access Management 11.1.2.2.0 Server login page. Upon successful authentication, it should perform a successful authorization and you should be able to access the resource successfully.

7

Migrating Completed Certifications From Oracle Identity Analytics to Oracle Identity Manager

This chapter describes how to migrate the closed certifications from Oracle Identity Analytics 11*g* Release 1 (11.1.1.5.0) to Oracle Identity Manager 11*g* Release 2 (11.1.2.2.0).

> **Note:** If you are using the earlier versions of Oracle Identity Analytics (for example, 11*g* Release 1 (11.1.1.3.0) or earlier), you must first upgrade Oracle Identity Analytics to 11*g* Release 1 (11.1.1.5.0), in order to migrate the closed certifications to Oracle Identity Manager 11*g* Release 2 (11.1.2.2.0).

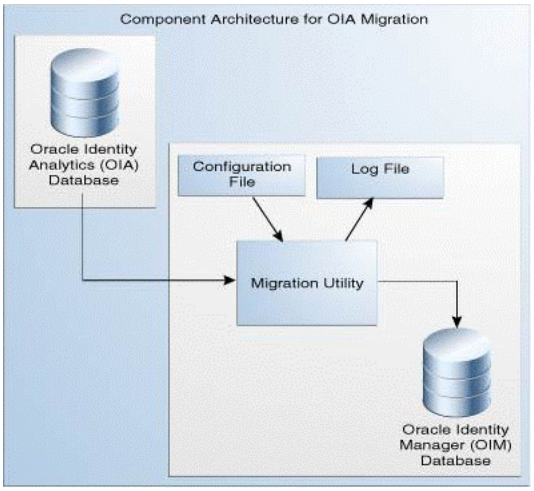
This chapter contains the following sections:

7.1 Migration Overview

The migration of closed certifications from Oracle Identity Analytics to Oracle Identity Manager can be done using the migration tool. The migration tool uses the database connection information provided in the properties file to connect to both Oracle Identity Analytics and Oracle Identity Manager databases, and migrates the certification data from Oracle Identity Analytics to Oracle Identity Manager.

Figure 7–1 illustrates the component architecture for Oracle Identity Analytics 11*g* Release 1 (11.1.1.5.0) migration.

Figure 7–1 Component Architecture for Oracle Identity Analytics Migration



To migrate the closed certifications from Oracle Identity Analytics to Oracle Identity Manager, you must have both Oracle Identity Analytics and Oracle Identity Manager running. When you invoke the migration utility, the migration tool connects to the Oracle Identity Analytics and Oracle Identity Manager databases using the database connection information provided in the `config.properties` file (referred to as Configuration File in Figure 7–1), and migrates the data. During migration, certification data from Oracle Identity Analytics database is read, processed, and written back to Oracle Identity Manager database. The migration tool generates a log file named `oiadatamigration.log` which contains the log information. After the migration completed successfully, all completed certifications in Oracle Identity Analytics are accessible via Oracle Identity Manager dashboard.

7.2 Migration Roadmap

Table 7–1 lists the tasks to be completed to migrate the closed certifications from Oracle Identity Analytics to Oracle Identity Manager.

Table 7–1 Roadmap for Migrating Closed Certifications from Oracle Identity Analytics to Oracle Identity Manager

Sl No	Task	For More Information,
1	Complete the prerequisites before starting the migration process.	See, Prerequisites for Migration
2	Obtain the migration tool (`oiaDataMigration.zip`).	See, Obtaining Migration Tool
3	Copy necessary `.jar` files from the Oracle Identity Analytics installation to the `lib` directory in the folder where you extracted the contents of `oiaDataMigration.zip` file.	See, Copying jar Files from Oracle Identity Analytics Installation
4	Specify the database connection details for Oracle Identity Analytics and Oracle Identity Manager in the `config.properties` file.	See, Specifying Database Connection Details

Table 7–1 (Cont.) Roadmap for Migrating Closed Certifications from Oracle Identity Analytics to Oracle Identity Manager

Sl No	Task	For More Information,
5	Migrate the closed certifications from Oracle Identity Analytics to Oracle Identity Manager by running the migration utility.	See, Migrating Closed Certifications
5	Verify the migration by checking the log file generated by the migration utility.	See, Verifying the Migration

7.3 Prerequisites for Migration

You must complete the following prerequisites before migrating closed certifications from Oracle Identity Analytics to Oracle Identity Manager 11.1.2.2.0:

- Read the system requirements and certification documents to ensure that your environment meets the minimum requirements for the products you are installing.
  - *Oracle Fusion Middleware System Requirements and Specifications*

    This document contains information related to hardware and software requirements, minimum disk space and memory requirements, and required system libraries, packages, or patches.
  - *Oracle Fusion Middleware Supported System Configurations*

    This document contains information related to supported installation types, platforms, operating systems, databases, JDKs, and third-party products.
  - For interoperability and compatibility issues that may arise when installing, refer to *Oracle Fusion Middleware Interoperability and Compatibility Guide*.

    This document contains important information regarding the ability of Oracle Fusion Middleware products to function with previous versions of other Oracle Fusion Middleware, Oracle, or third-party products. This information is applicable to both new Oracle Fusion Middleware users and existing users who are upgrading their existing environment.

    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*.
- Make sure that you have installed and configured Oracle Identity Manager 11.1.2.2.0. Both Oracle Identity Analytics and Oracle Identity Manager should be running in order to perform this migration.

7.4 Obtaining Migration Tool

The migration toolkit is available as a zip file named `oiaDataMigration.zip`. Contact Oracle Support to obtain the migration tool.

Extract the files of `oiaDataMigration.zip` to a location of your choice. `oiaDataMigration.zip` folder contains the following directories.

- `config`: This directory contains a properties file called `config.properties`, which contains the database connection information for Oracle Identity Analytics and Oracle Identity Manager.
- `lib`: This is an empty directory. You must copy certain jar files present in your Oracle Identity Analytics installation to this directory. The list of jar files that you must copy to this folder is listed in Section 7.5, "Copying jar Files from Oracle Identity Analytics Installation".
- `logs`: This directory contains the log files created by the migration utility.
- `oiaDataMigration.jar`: This is the executable migration utility which migrates closed certifications from Oracle Identity Analytics to Oracle Identity Manager.
- `readme.txt`: This file contains information about the release and how to use the migration utility.

7.5 Copying jar Files from Oracle Identity Analytics Installation

Copy the following `.jar` files from the existing Oracle Identity Analytics installation to the location *<unzipped_folder_of_oiaDataMigration.zip>*`/lib`:

- `aopalliance.jar`
- `commons-collections-3.1.jar*`
- `commons-collections-3.2.1.jar*`
- `commons-dbcp.jar*`
- `commons-logging-1.1.jar*`
- `commons-logging.jar*`
- `commons-pool-1.2.jar*`
- `commons-pool-1.3.jar*`
- `log4j-1.2.14.jar*`
- `ojdbc6.jar*`
- `spring-aop.jar`
- `spring-beans.jar`
- `spring-context.jar`
- `spring-core.jar`
- `spring-jdbc.jar`
- `spring-tx.jar`

7.6 Specifying Database Connection Details

Before you run the migration utility, you must specify the database connection details for Oracle Identity Analytics and Oracle Identity Manager in the `config.properties` file. To do this, complete the following steps:

1. Open the `config.properties` file from the location *<folder_where_you_unzipped_oiaDataMigration.zip>*`/config/` in a text editor.
2. Specify the appropriate values for the following parameters:
   - `oia.jdbc.url`: Specify the JDBC URL for Oracle Identity Analytics.

- `oia.jdbc.username`: Specify the Oracle Identity Analytics JDBC username.
- `oim.jdbc.url`: Specify the JDBC URL for Oracle Identity Manager 11.1.2.2.0.
- `oim.jdbc.username`: Specify the Oracle Identity Manager JDBC username.
- `logging.level`: Specify the level of details you wish to have in the log file generated by the migration utility. Specify one of the following values for this parameter:
  - `DEBUG` - Specify this value for information about debugging.
  - `INFO` - Specify this value for general information.
  - `WARN` - Specify this value for warning messages.
  - `ERROR` - Specify this value for error messages.

Sample properties file:

```
#oia parameters

oia.jdbc.url = jdbc:oracle:thin:@$SERVER_NAME:$PORT:rbacx
oia.jdbc.username=oiadbuser

#oim paramters

oim.jdbc.url = jdbc:oracle:thin:@$SERVER_NAME:$PORT:oimdb
oim.jdbc.username=oimdbuser

# could be one of DEBUG,INFO,WARN,ERROR.
logging.level = WARN
```

3. Save the `config.properties` file.

7.7 Migrating Closed Certifications

Run the migration tool to migrate the closed certifications Oracle Identity Analytics to Oracle Identity Manager by doing the following:

1. Go to the location where you extracted the files of `oiaDataMigration.zip`.
2. Run the `oiaDataMigration.jar` file as shown below:

   ```
   java -jar oiaDataMigration.jar -<option>
   ```

   In this command, *<option>* refers to the option that you must use while running the `oiaDataMigration.jar` command depending on the task you wish to perform. Table 7–2 lists the options that can be used while running the `oiaDataMigration.jar` command:

Table 7–2 Options to be Used While Running oiaDataMigration.jar Command

Option	Description	For Example,
`-all`	Use this option if you wish to migrate all the closed certifications from Oracle Identity Analytics to Oracle Identity Manager 11.1.2.2.0. This option is incompatible with the option `-range`.	`java -jar oiaDataMigration.jar -all`

Table 7–2 (Cont.) Options to be Used While Running oiaDataMigration.jar Command

Option	Description	For Example,
`-purge`	Use this option if you wish to remove all completed certification data that was migrated from Oracle Identity Analytics to Oracle Identity Manager 11.1.2.2.0. This also removes any certification data generated from Oracle Identity Manager.	`java -jar oiaDataMigration.jar -purge`
`-range start <MM/DD/YYYY> end <MM/DD/YYYY>`	Use this option if you wish to migrate a set of closed certifications who date of completions fall under a certain period. When using this option, you must mention the start date and end date of the period.	`java -jar oiaDataMigration.jar -range start 01/01/2012 end 03/31/2012`
`-stats`	Use this option if you wish to compare the certification data in Oracle Identity Analytics with the certification data in Oracle Identity Manager.	`java -jar oiaDataMigration.jar -stats`
`-help`	Use this option for more information about how to run the `oiaDataMigration.jar` command.	`java -jar oiaDataMigration.jar -help`

3. Specify the password for Oracle Identity Analytics and Oracle Identity Manager databases, when prompted.

This migrates the closed certifications from Oracle Identity Analytics to Oracle Identity Manager.

7.8 Verifying the Migration

After the migration is completed, verify that the specified data was migrated correctly by running the migration tool again using the `-stats` option as follows:

```
java -jar oiaDataMigration.jar -stats
```

> **Note:** For more information about running the migration tool, see Section 7.7, "Migrating Closed Certifications".

The output displays the number of records found in each Oracle Identity Analytics table and each Oracle Identity Manager table. If the migration was successful, the values in each column will be equal.

You can also check the log file `oiadatamigration.log` generated at the location `<folder_where_you_unzipped_oiaDataMigration.zip>/logs/` for any errors or warnings.

Part III

Coexistence Scenarios

This part includes the following chapters:

8

Coexistence of Oracle Access Manager 10*g* with Oracle Access Management Access Manager 11.1.2.2.0

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 (11.1.2.2.0) deployments coexist.

This chapter contains the following sections:

8.1 Coexistence Overview

Both Oracle Access Manager 10*g* and Access Manager 11.1.2.2.0 deployments can coexist, so that some applications are protected by Oracle Access Manager 10*g* while others are protected by Access Manager 11.1.2.2.0. This is called Coexistence mode, where both Oracle Access Manager 10*g* and Access Manager 11.1.2.2.0 deployments coexist.

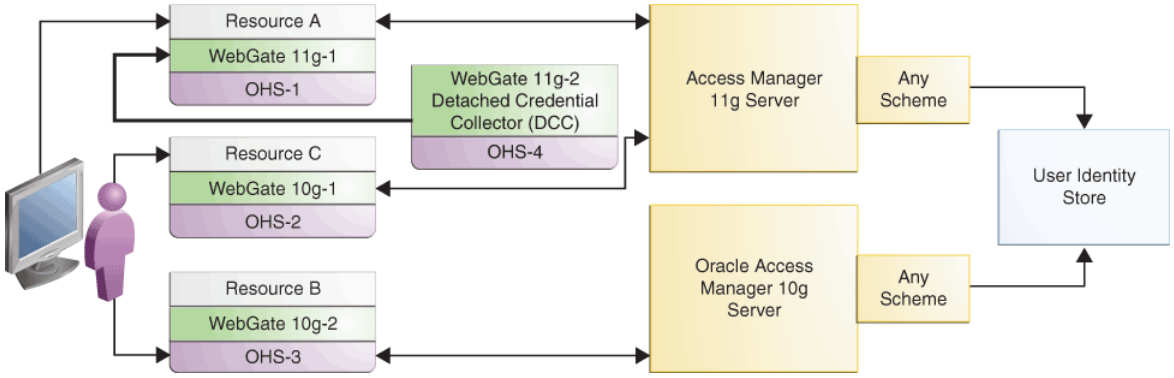
In the Coexistence mode, Access Manager 11.1.2.2.0 protects the migrated applications and any new applications registered with Access Manager 11.1.2.2.0; whereas Oracle Access Manager 10*g* continues to protect the applications that are not migrated to Access Manager 11.1.2.2.0.

End-users have a seamless single sign-on (SSO) experience when they navigate between applications that are protected by Oracle Access Manager 10*g* and applications protected by Access Manager 11.1.2.2.0.

8.2 Coexistence Features

Figure 8–1 illustrates how Oracle Access Manager 10*g* Server coexists with Access Manager 11.1.2.2.0 Server. Resource A is protected by Access Manager 11*g* WebGate and the other resources are protected by Oracle Access Manager 10*g* WebGates. You can configure Oracle Access Manager 10*g* WebGates to work with either Oracle Access Manager 10*g* server or Access Manager 11.1.2.2.0 server; Access Manager 11*g* WebGate can be configured to work with Access Manager 11.1.2.2.0 server only.

Figure 8–1 Coexistence of Oracle Access Manager 10g with Access Manager 11.1.2.2.0



- Oracle Access Manager 10*g* and Access Manager 11.1.2.2.0 Servers can independently handle all authentication and authorization requests that are routed to them, without depending on each other.
- All authentication schemes and policies are preserved during coexistence. This applies for both existing applications protected by Oracle Access Manager 10*g* and the migrated applications protected by the Access Manager 11.1.2.2.0 platform. For example, if an application is protected by X509 authentication scheme, then it is protected by X509 authentication scheme even in the Access Manager 11.1.2.2.0 platform, during coexistence.
- Users authenticated by Access Manager 11.1.2.2.0 Server need not enter credentials again if they access any resource protected by Oracle Access Manager 10*g* server and vice versa. This provides users a seamless single sign-on (SSO) experience. A user can access resource B protected by Oracle Access Manager 10*g* and then access resource A protected by Access Manager 11.1.2.2.0 without entering the user credentials again.
- Only one session is created per user, so you cannot use session management feature in Coexistence mode.
- If a user logs out from any one of the servers, the session ends and the user is logged out from both Access Manager 11.1.2.2.0 and Oracle Access Manager 10*g* servers. A user can access any protected resource only after re-authentication.
- Users can leverage all authentication related features and enhancements of Access Manager 11.1.2.2.0 in Coexistence mode. For more information about enhancements in Oracle Access Manager 11.1.2.2.0, see "Product Enhancements for

Oracle Access Management 11.1.2.2.0" in Oracle Fusion Middleware Administrator's Guide for Oracle Access Management.

- Authentication level for all protected resources must be the same, irrespective of the authentication scheme. In Figure 8–1, Resources A, B, and C must have the same authentication level, otherwise user will need to enter credentials again while trying to access resources having different authentication levels.
- In Coexistence mode, no settings are required on the Access Manager 11*g* server to enable SSO across multiple data centers (MDC). The ObSSOCookie, which is generated by both Access Manager 11*g* server and Oracle Access Manager 10*g* server, is used as the source of user authorization. Plain 10*g* MDC mode is supported in Coexistence mode where cookie validation is the only criteria for a valid user session. If user session is not present in any data center, a new session is created irrespective of the existing session in other data center. For more information about deploying MDC, see "Using Multi-Data Centers" in Oracle Fusion Middleware Administrator's Guide for Oracle Access Management.

8.2.1 About Credential Collection

Access Manager 11.1.2.2.0 Server provides two mechanisms for collecting credentials during authentication processing:

- Embedded Credential Collector (ECC). The default ECC is installed with the Access Manager Server and can be used as-is with no additional installation or set up steps. For more information about collecting and processing user credentials with ECC, see "About SSO Login Processing with OAM Agents and ECC" in Oracle Fusion Middleware Administrator's Guide for Oracle Access Management.
- Separate Detached Credential Collector (DCC) and Resource WebGate. This is a distributed deployment where WebGates protecting applications are managed independently from the centralized DCC. The Resource WebGate which protects the resource redirects the user request to the DCC-enabled 11*g* WebGate for authentication. For more information about collecting and processing user credentials with DCC, see "About Login Processing with OAM Agents and DCC" in Oracle Fusion Middleware Administrator's Guide for Oracle Access Management.

Table 8–1 provides a comparison of the mechanisms used for collecting credentials in Coexistence Mode by WebGate 11*g* and WebGate 10*g* registered with Access Manager 11.1.2.2.0 Server.

Table 8–1 Comparison: WebGate 11g versus WebGate 10g with Access Manager 11g

	11*g* WebGate	**10*g* WebGate**
ECC	Does not support ECC for collecting credentials.	Supports ECC for collecting credentials.
DCC	Requires a DCC-enabled 11*g* WebGate, which is separate from an 11*g* Resource WebGate, to work in Coexistence Mode.	Requires ECC or a DCC-enabled 11*g* WebGate.

Table 8–2 provides a comparison of the mechanisms used for collecting credentials by WebGate 10*g* in 10*g* and 11*g* deployments. For more differences between installing a 10*g* Webgate to operate in an 11*g* Access Manager deployment versus installing the 10*g* Webgate in an 10*g* Oracle Access Manager deployment, see "Table 23-1 Installation Comparison with 10*g* Webgates" in *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.

Table 8–2 Comparison: WebGate 10g in 11g Deployment versus 10g Deployment

	10*g* WebGate in 11*g* Deployment	10*g* WebGate in 10*g* Deployment
Login Form	You cannot use 10*g* forms provided with 10*g* WebGates with Access Manager Server. Using 10*g* WebGates with Access Manager Server is similar in operation and scope to a resource WebGate (one that redirects in contrast to the Authentication WebGate). With a 10*g* WebGate and 11*g* OAM Server, the 10*g* WebGate always redirects to the 11*g* credential collector which acts like the Authenticating WebGate.	You can use the 10*g* forms which were provided for use in 10*g* deployments.

8.3 Coexistence Topology

Figure 8–1 illustrates how Oracle Access Manager 10*g* Server coexists with Access Manager 11.1.2.2.0 Server.

The topology consists of disjoint Oracle Access Manager 10*g* and Access Manager 11.1.2.2.0 setups where resources, WebGates, and servers are in the same domain.

This coexistence setup contains the following:

- Oracle Access Manager 10*g* WebGate partners registered against Access Manager 11.1.2.2.0 Server. To enable coexistence, configure Oracle Access Manager 10*g* WebGate with DCC or ECC in 11*g* Access Manager.
- Oracle Access Manager 10*g* WebGate partners registered against Oracle Access Manager 10*g* Server.
- Access Manager 11*g* WebGate partners registered against Access Manager 11.1.2.2.0 Server.

Topology Description

- `WebGate 11g-1`: This refers to the 11*g* WebGate partner registered with Access Manager 11.1.2.2.0 Server. It is deployed on Oracle HTTP Server 11*g* named `OHS-1`. `WebGate 11g-1` protects Resource A, an application that is installed on Access Manager 11.1.2.2.0 Server. 11*g* WebGates work only with Access Manager 11.1.2.2.0 Server. To enable 11*g* WebGate to work in coexistence mode, you must configure the 11*g* WebGate to work with a detached credential collector (DCC).
- `WebGate 11g-2`: This refers to the 11*g* WebGate configured as a detached credential collector (DCC). An 11*g* WebGate configured to act as a detached credential collector (DCC) is known as an Authenticating WebGate. The other 11*g* WebGate, WebGate 11*g*-1, which protects resources, is called Resource WebGate. WebGate 11*g*-1 and WebGate 11*g*-2 work together in coexistence mode as separate DCC and Resource WebGates.

  The Resource WebGate does not communicate directly with the Access Manager 11.1.2.2.0 Server. Access Manager 11.1.2.2.0 Server receives requests from the Resource WebGate and redirects authentication requests to the DCC. The DCC sets the ObSSOCookie for the session, which is honored by both the Access Manager 11.1.2.2.0 Server and Oracle Access Manager 10*g* Server. For information about configuring 11*g* WebGates as Separate DCC and Resource WebGates, see "Configuring 11*g* Webgate and Authentication Policy for DCC" in Oracle Fusion Middleware Administrator's Guide for Oracle Access Management.
- `WebGate 10g-1`: This refers to the Oracle Access Manager 10*g* WebGate partner registered with Access Manager 11.1.2.2.0 Server. It is deployed on Oracle HTTP

Server 11*g* named `OHS-2.WebGate 10g-1` protects Resource C, an application that is installed on Access Manager 11.1.2.2.0 server.

- `WebGate 10g-2`: This refers to the Oracle Access Manager 10*g* WebGate partner registered with Oracle Access Manager 10*g* Server. It is deployed on Oracle HTTP Server 11*g* named `OHS-3.WebGate 10g-2` protects Resource B, an application that is protected by Oracle Access Manager 10*g*.
- User Identity Store: Access Manager 11.1.2.2.0 Server and Oracle Access Manager 10*g* Server are configured to share the same user identity store, so that both the servers can validate and update the ObSSOCookie, which is present in the user request.

The following scenarios explain how SSO works in Coexistence mode when user accesses resources that are protected by Access Manager 11.1.2.2.0 Server and Oracle Access Manager 10*g* Server:

- Section 8.3.1, "Accessing resource protected by 10g WebGate and Oracle Access Manager 10g and then accessing resource protected by 10g WebGate and Access Manager 11g"
- Section 8.3.2, "Accessing resource protected by 11g WebGate and Access Manager 11g and then accessing resource protected by 10g WebGate and Oracle Access Manager 10g"
- Section 8.3.3, "Accessing resource protected by 10g WebGate and Access Manager 10g and then accessing resource protected by 11g WebGate and Access Manager 11g"
- Section 8.3.4, "Accessing resource protected by 10g WebGate and Access Manager 11g and then accessing resource protected by 11g WebGate and Access Manager 11g"

8.3.1 Accessing resource protected by 10*g* WebGate and Oracle Access Manager 10*g* and then accessing resource protected by 10*g* WebGate and Access Manager 11*g*

In the coexistence mode, if a user has already been authenticated by Oracle Access Manager 10*g* Server, the Access Manager 11.1.2.2.0 Server honors the ObSSOCookie set by Oracle Access Manager 10*g* Server and creates a unified session. Hence, the user does not need to enter credentials again.

Figure 8–2 illustrates how SSO works in the coexistence mode when a user accesses Resource B which is protected by WebGate 10*g*-2 registered against Oracle Access Manager 10*g* Server, and then accesses Resource C which is protected by WebGate 10*g*-1 registered against Access Manager 11.1.2.2.0 Server.

Figure 8–2 User accesses Resource B protected by 10g WebGate and Oracle Access Manager 10g and then tries to access Resource C protected by 10g WebGate and Access Manager 11g

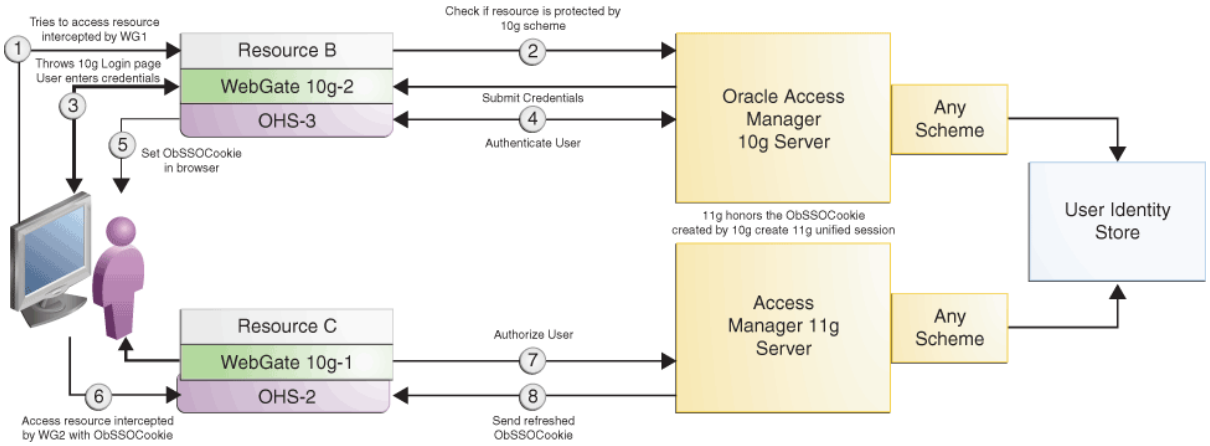


Table 8–3 describes the request flow. The numbers in the **Step** column correspond to the numbers shown in the topology in Figure 8–2 and show the sequence in which the requests flow in the coexistence environment.

Table 8–3 Request Flow

Step	Description
1	User requests access to `Resource-B`, which is protected by Oracle Access Manager 10*g* Server at the following URL: `http://OHS-3:port/ResourceB` where `OHS-3` is the hostname of the Oracle HTTP Server 10*g* (`OHS-3`), and the `port` is the port number of the machine on which `OHS-3` is running.
2	`WebGate 10g-2` which is deployed on `OHS-3` intercepts the request, and communicates with the Oracle Access Manager 10*g* Server to authenticate the user.
3	`WebGate 10g-2` redirects the user to a login form to collect the credentials.
4 and 5	When the user provides the credentials, `WebGate 10g-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 and ObSSOCookie to `WebGate 10g-2` according to the policy configuration. `WebGate 10g-2` sets the ObSSOCookie in the user's browser.
6	User requests access to `Resource-C`, which is protected by Access Manager 11.1.2.2.0 Server at the following URL: `http://OHS-2:port/ResourceC` where `OHS-2` is the hostname of the Oracle HTTP Server 11*g* (`OHS-2`), and the `port` is the port number of the machine on which `OHS-2` is running. The request contains the ObSSOCookie set in the header by `WebGate 10g-2`.
7-8	Access Manager 11.1.2.2.0 server validates the ObSSOCookie, authorizes the user, creates a unified session, and sends the refreshed ObSSOCookie to `WebGate 10g-1` according to the policy configuration.

8.3.2 Accessing resource protected by 11*g* WebGate and Access Manager 11*g* and then accessing resource protected by 10*g* WebGate and Oracle Access Manager 10*g*

Figure 8–3 illustrates how SSO works in the coexistence mode when a user accesses Resource A protected by Access Manager 11.1.2.2.0 Server, and then accesses Resource B protected by the Oracle Access Manager 10*g* Server.

Figure 8–3 User accesses Resource A protected by 11g WebGate and Access Manager 11g Server and then tries to access Resource C protected by 10g WebGate and Oracle Access Manager 10g Server

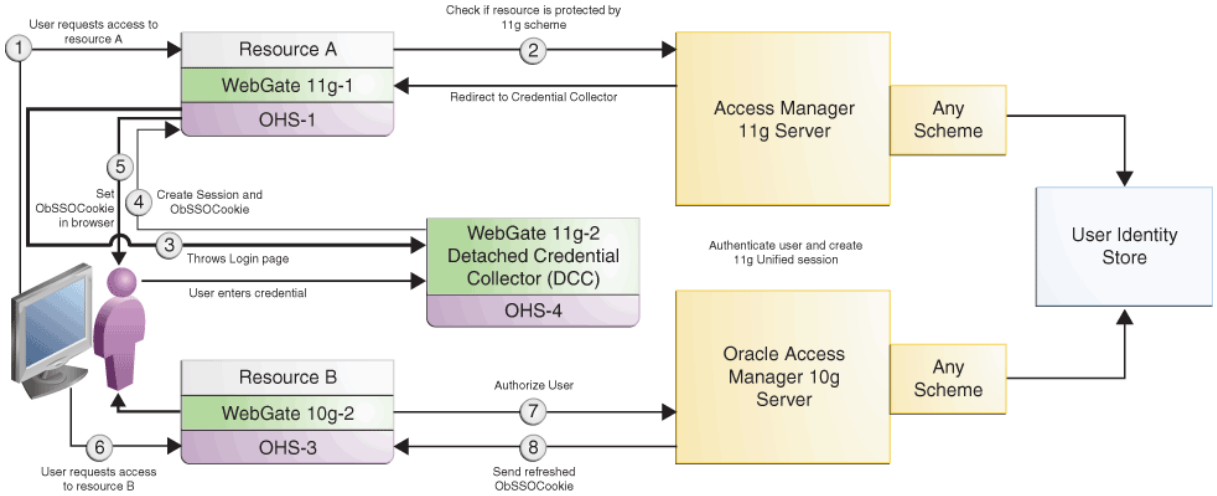


Table 8–4 describes the request flow. The numbers in the **Step** column correspond to the numbers shown in the topology in Figure 8–3 and show the sequence in which the requests flow in the coexistence environment.

Table 8–4 Request Flow

Step	Description
1	User requests access to `Resource-A`, which is protected by Access Manager 11.1.2.2.0 Server at the following URL: `http://OHS-1:port/ResourceA` 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	`WebGate 11g-1` which is deployed on `OHS-1` intercepts the request and communicates with Access Manager 11.1.2.2.0 Server to obtain the authentication scheme.
3	Access Manager 11.1.2.2.0 Server redirects the request to the detached credential collector (DCC), which throws the login page. The DCC collects and processes the credentials entered by the user for authentication.
4-5	When user provides the credentials, the detached credential collector communicates with Access Manager 11.1.2.2.0 Server to perform authentication followed by authorization. After authorization, the Access Manager 11.1.2.2.0 server provides all relevant headers and ObSSOCookie to `WebGate 11g-1` according to the policy configuration. ObSSOCookie is generated as per Oracle Access Manager 10*g* Server specifications, and `WebGate 11g-1` sets the ObSSOCookie in the user's browser.

Table 8–4 (Cont.) Request Flow

Step	Description
6	User requests access to `Resource-B`, which is protected by Oracle Access Manager 10*g* Server, at the following URL: `http://OHS-2:port/ResourceB` where `OHS-2` is the hostname of the Oracle HTTP Server 10*g* (`OHS-2`), and the `port` is the port number of the machine on which `OHS-2` is running. The request contains the ObSSOCookie set in the header by `WebGate 11g-1`.
7-8	Oracle Access Manager 10*g* Server decrypts and validates the ObSSOCookie, authorizes the user, and sends the refreshed ObSSOCookie to `WebGate10g-2` according to the policy configuration.

In the coexistence mode, Access Manager 11.1.2.2.0 Server redirects the user request to a credential collector to collect credentials for both 10*g* and 11*g* WebGates. For comparison of the mechanisms used for collecting credentials in Coexistence mode by WebGate 11*g* and WebGate 10*g*, see Section 8.2.1, "About Credential Collection".

8.3.3 Accessing resource protected by 10*g* WebGate and Access Manager 10*g* and then accessing resource protected by 11*g* WebGate and Access Manager 11*g*

Figure 8–4 illustrates how SSO works in the coexistence mode when a user accesses Resource B protected by Oracle Access Manager 10*g* Server, and then accesses Resource A protected by Access Manager 11.1.2.2.0 Server.

Figure 8–4 User accesses Resource B protected by 10g WebGate and Access Manager 10g Server and then tries to access Resource A protected by 11g WebGate and Access Manager 11g Server

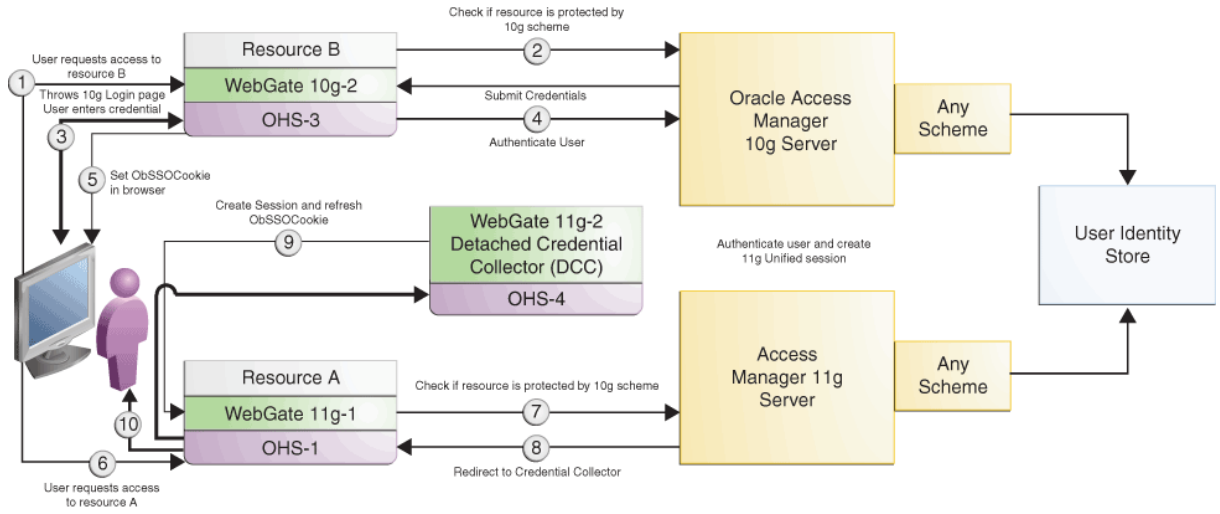


Table 8–5 describes the request flow. The numbers in the **Step** column correspond to the numbers shown in the topology in Figure 8–4 and show the sequence in which the requests flow in the coexistence environment.

Table 8–5 Request Flow

Step	Description
1	User requests access to `Resource-B`, which is protected by Oracle Access Manager 10*g* Server at the following URL: `http://OHS-3:port/ResourceB` where `OHS-3` is the hostname of the Oracle HTTP Server 10*g* (`OHS-3`), and the `port` is the port number of the machine on which `OHS-3` is running.
2	`WebGate 10g-2` which is deployed on `OHS-3` intercepts the request, and communicates with the Oracle Access Manager 10*g* Server to authenticate the user.
3	`WebGate 10g-2` redirects the user to a login form to collect the credentials.
4 and 5	When the user provides the credentials, `WebGate 10g-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 and ObSSOCookie to `WebGate 10g-2` according to the policy configuration, and these are then set by the WebGate. `WebGate 10g-2` sets the ObSSOCookie in the user's browser.
6	User requests access to `Resource-A`, which is protected by Access Manager 11.1.2.2.0 Server at the following URL: `http://OHS-1:port/ResourceA` where `OHS-1` is the hostname of the Oracle HTTP Server 11*g* (`OHS-2`), and the `port` is the port number of the machine on which `OHS-1` is running. The request contains the ObSSOCookie set in the header by `WebGate 10g-2`.
7	`WebGate 11g-1` which is deployed on `OHS-1` intercepts the request, and communicates with Access Manager 11.1.2.2.0 Server to obtain the authentication scheme.
8	Access Manager 11.1.2.2.0 Server redirects the request to the DCC along with the ObSSOCookie set by `WebGate 10g-2`.
9-10	DCC communicates with Access Manager 11.1.2.2.0 Server to perform authentication followed by authorization. After authorization, the Access Manager 11.1.2.2.0 server sends the refreshed ObSSOCookie to `WebGate 11g-1` according to the policy configuration.

8.3.4 Accessing resource protected by 10*g* WebGate and Access Manager 11*g* and then accessing resource protected by 11*g* WebGate and Access Manager 11*g*

Figure 8–5 illustrates how SSO works in the coexistence mode when a user accesses Resource C protected by Access Manager 11.1.2.2.0 Server, and then accesses Resource A protected by the Access Manager 11.1.2.2.0 Server.

Figure 8–5 User accesses Resource C protected by 10g WebGate and Access Manager 11g Server and then tries to access Resource A protected by 11g WebGate and Access Manager 11g Server

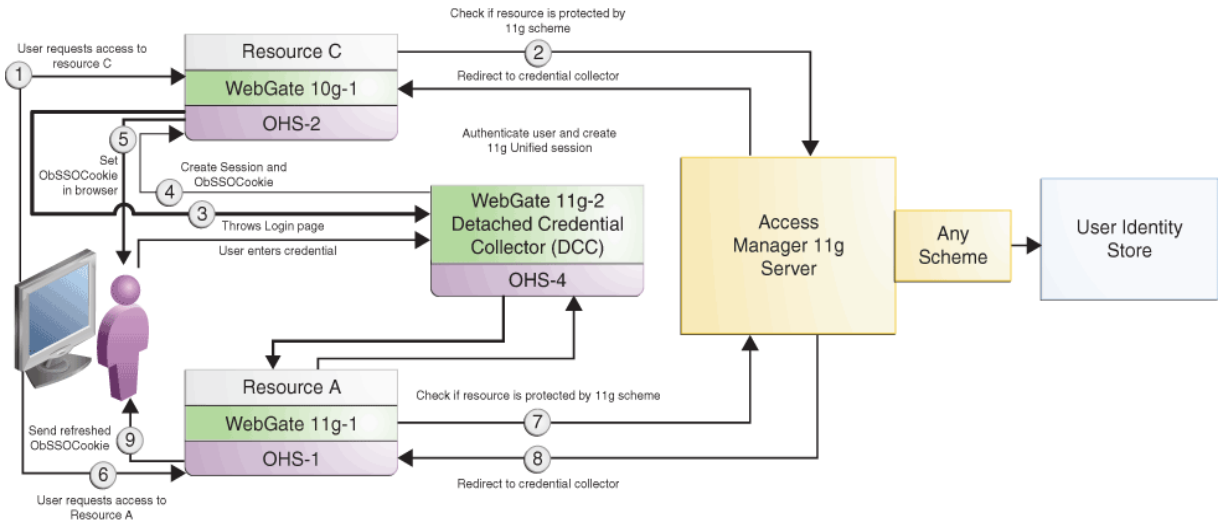


Table 8–6 describes the request flow. The numbers in the **Step** column correspond to the numbers shown in the topology in Figure 8–5 and show the sequence in which the requests flow in the coexistence environment.

Table 8–6 Request Flow

Step	Description
1	User requests access to `Resource-C`, which is protected by Access Manager 11.1.2.2.0 Server at the following URL: `http://OHS-2:port/ResourceC` where `OHS-2` is the hostname of the Oracle HTTP Server 10*g* (`OHS-2`), and the `port` is the port number of the machine on which `OHS-2` is running.
2	`WebGate 10g-1` which is deployed on `OHS-2` intercepts the request, and communicates with Access Manager 11.1.2.2.0 Server to obtain the authentication scheme.
3	Access Manager 11.1.2.2.0 Server redirects the request to the ECC or DCC, which throws the login page. The ECC or DCC collects and processes the credentials entered by the user for authentication.
4-5	When user provides the credentials, the ECC or DCC communicates with Access Manager 11.1.2.2.0 Server to perform authentication followed by authorization. After authorization, the Access Manager 11.1.2.2.0 server provides all relevant headers and ObSSOCookie to `WebGate 10g-1` according to the policy configuration. `WebGate 10g-1` sets the ObSSOCookie in the user's browser.
6	User requests access to `Resource-A`, which is protected by Access Manager 11.1.2.2.0 Server at the following URL: `http://OHS-1:port/ResourceA` where `OHS-1` is the hostname of the Oracle HTTP Server 11*g* (`OHS-1`), and the `port` is the port number of the ma chine on which `OHS-1` is running. The request contains the ObSSOCookie set in the header by `WebGate 10g-1`.
7	`WebGate 11g-1` which is deployed on `OHS-1` intercepts the request, and communicates with Access Manager 11.1.2.2.0 Server to obtain the authentication scheme.

Table 8–6 (Cont.) Request Flow

Step	Description
8	Access Manager 11.1.2.2.0 Server redirects the request to the DCC along with the ObSSOCookie set by WebGate 10*g*-1.
9	DCC communicates with Access Manager 11.1.2.2.0 Server to perform authentication followed by authorization. After authorization, the Access Manager 11.1.2.2.0 server sends the refreshed ObSSOCookie to WebGate 11*g*-1 according to the policy configuration.

8.4 Task Roadmap

Table 8–7 lists the steps to set up and configure the topology shown in Figure 8–1.

Table 8–7 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 a new Oracle HTTP Server 11*g* instance (`OHS-1`). If you do not want to install a new Oracle HTTP Server instance, 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)
4	Install a new 11*g* WebGate and configure it to work with Access Manager 11.1.2.2.0 Server and DCC. `WebGate 11g-1` is deployed on `OHS-1` and configured with Access Manager 11.1.2.2.0 Server.	See Optional: Installing and Configuring WebGate 11g-1
5	Use the existing 10*g* Webgares or install three WebGates: `WebGate 10g-1 and WebGate 10g-2`. You can install 10*g* or 11*g* WebGates. You can configure 10*g* WebGates to work with Access Manager 11.1.2.2.0 Server or Oracle Access Manager 10*g* Server. You can configure 11*g* WebGates to work only with Access Manager 11.1.2.2.0 Server. `WebGate 10g-1` is deployed on `OHS-2` and configured with Access Manager 11.1.2.2.0 Server. `WebGate 10g-2` is deployed on `OHS-3` and configured with Oracle Access Manager 10*g* Server. This WebGate must be a 10*g* WebGate.	See Optional: Installing and Configuring 10g WebGates
6	Enable coexistence mode on the Access Manager 11.1.2.2.0 Server	See Enabling Coexistence Mode on Access Manager 11.1.2.2.0 Server
7	Configure the logout settings to ensure that the logout works at both the WebGates and the Access Manager 11.1.2.2.0 server.	See Configuring Logout Settings
8	Verify the configuration.	See Verifying the Configuration

8.5 Prerequisites for Coexistence

You must complete the following prerequisites before you start performing tasks required for coexistence of Oracle Access Manager 10*g* Server with Access Manager 11.1.2.2.0 Server.

1. Read the system requirements and certification documents to ensure that your environment meets the minimum requirements for the products you are installing.

   - *Oracle Fusion Middleware System Requirements and Specifications*

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

   - *Oracle Fusion Middleware Supported System Configurations*

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

   - For interoperability and compatibility issues that may arise when installing, refer to *Oracle Fusion Middleware Interoperability and Compatibility Guide*.

     This document contains important information regarding the ability of Oracle Fusion Middleware products to function with previous versions of other Oracle Fusion Middleware, Oracle, or third-party products. This information is applicable to both new Oracle Fusion Middleware users and existing users who are upgrading their existing environment.

     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 supports coexistence. For more information about supported starting points for coexistence of Oracle Access Manager 10*g* with Access Manager 11.1.2.2.0, see Section 1.4, "Supported Starting Points for Migration and Coexistence".
3. Ensure that the Oracle Access Manager 10*g* and the Access Manager 11.1.2.2.0 servers are up and running.
4. Configure user identity store in Access Manager 11.1.2.2.0. For more information about configuring user identity store, see Section 8.5.1, "Configuring User Identity Store in Access Manager 11.1.2.2.0".
5. Install JDK 6 or JDK 7 on all the Access Manager 11.1.2.2.0 servers that you want to run in coexistence mode with Oracle Access Manager 10*g* servers.
6. Download the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 7 from the Oracle Technology Network website at `http://www.oracle.com/technetwork/java/javase/downloads/jce-7-download-432124.html` and place the `US_export_policy.jar` and `local_policy.jar` files in the `jre/lib/security` folder.

8.5.1 Configuring User Identity Store in Access Manager 11.1.2.2.0

While configuring the User Identity Store in Access Manager 11.1.2.2.0, you need to complete the following tasks:

- Set Access Manager 11.1.2.2.0 Server as a default store.
- Ensure that Oracle Access Manager 10*g* and Access Manager 11.1.2.2.0 servers share the same user store.
- Mark the shared data store as the default data store.
- Select the shared data store under LDAP Authentication Module.

To do this, complete the following steps:

1. Log in to the Oracle Access Management 11.1.2.2.0 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 11.1.2.2.0 console, which is the same as the bind port for the Administration Server.
2. Under Configuration, click **User Identity Stores**.
3. Create a User Identity Store, whose location or host information points to the Access Manager 11.1.2.2.0 server. For more information about creating a user identity store, see "Registering a New User Identity Store" in Oracle Fusion Middleware Administrator's Guide for Oracle Access Management.
4. On the User Identity Stores page, under Default and System store, select the user identity store you have created.
5. Click **Apply**.
6. On the Oracle Access Management Launch Pad, under Access Manager, click **Authentication Modules**. A list of authentication modules appears.
7. Click **LDAP** and update the User Identity Store to point to the user identity store that you have just created.
8. Click **Apply**.

8.6 Optional: Installing and Configuring Oracle HTTP Server 11*g* (OHS-1)

Install and configure Oracle HTTP Server 11*g* (`OHS-1` as shown in Figure 8–1). Alternatively, you can use the Oracle HTTP Server instances that exist after migration from Oracle Access Manager 10*g* to Access Manager 11.1.2.2.0.

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

You can install 11*g* WebGate on the following web servers: Oracle HTTP Server (OHS), Oracle Traffic Director, and Apache 2. In the sample topology which we consider in this chapter, all WebGates are considered to be installed on OHS.

8.7 Optional: Installing and Configuring WebGate 11*g*-1

To enable 11*g* WebGates to work in coexistence mode, you must configure the 11*g* Resource WebGate to work with a DCC-enabled 11*g* WebGate as Separate DCC and Resource WebGates.

- Install and configure an 11*g* WebGate, which protects resources, to work with the DCC. This WebGate is called the Resource WebGate. Access Manager 11.1.2.2.0 server redirects the authentication requests it receives from the Resource WebGate to the DCC to collect and process authentication. Install a new 11*g* WebGate instance on Oracle HTTP Server 11*g* (`OHS-1`), as shown in Figure 8–1, and configure it with the Access Manager 11.1.2.2.0 Server. For information about installing 11*g* WebGate and configuring it with the Access Manager 11.1.2.2.0 server, see "Installing and Configuring Oracle HTTP Server 11*g* WebGate for OAM" in the *Oracle Fusion Middleware Installing WebGates for Oracle Access Manager*.
- Install and configure an 11*g* WebGate to act as a detached credential collector (DCC). This WebGate is also known as an Authenticating WebGate. For information about configuring 11*g* WebGates as Separate DCC and Resource WebGate, see "Configuring 11*g* WebGate and Authentication Policy for DCC" in the Oracle Fusion Middleware Administrator's Guide for Oracle Access Management.

> **Note:** The DCC must be in the same domain as the Authenticating WebGate of Oracle Access Manager 10*g* Server, so that the ObSSOCookie can be passed to both WebGates.

8.8 Optional: Installing and Configuring 10*g* WebGates

You can either use existing 10*g* WebGate instances for setting up the coexistence environment or install new 10*g* WebGate instances.

If you want to install new WebGates instances: `WebGates 10g-1` and `WebGates 10g-2`, you must configure them as follows:

- `WebGate 10g-1`: Install a 10*g* WebGate on Oracle HTTP Server 11*g* (`OHS-2`), as shown in Figure 8–1, and configure it with the Access Manager 11.1.2.2.0 Server.

  For information about installing 10*g* WebGate, and configuring it with the Access Manager 11.1.2.2.0 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*.

  When you use a 10*g* WebGate with Access Manager 11.1.2.2.0 Server, the 10*g* WebGate behaves as a Resource WebGate and always redirects to the 11*g* credential collector which acts as the Authenticating WebGate. You can configure 10*g* WebGates to work with the default Embedded Credential Collector (ECC) that is installed with the Access Manager 11.1.2.2.0 Server or a 11*g* WebGate configured as a Detached Credential Collector (DCC). For more information about ECC and DCC, see "Introduction to Access Manager Credential Collection and Login" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.
- `WebGate 10g-2`: Install a 10*g* WebGate on Oracle HTTP Server 11*g* (`OHS-2`), as shown in Figure 8–1, and configure it with the Oracle Access Manager 10*g* Server.

  For information about 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).

For more information about managing 10*g* WebGates with Access Manager 11.1.2.2.0, see "Managing 10*g* WebGates with Oracle Access Manager 11*g*" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.

Note: All 10*g* WebGates configured with Oracle Access Manager 10*g* Server or Access Manager 11.1.2.2.0 Server should have the same primary cookie domain otherwise ObSSOCookie cannot be passed from one WebGate to another.

8.9 Enabling Coexistence Mode on Access Manager 11.1.2.2.0 Server

Run the following WebLogic Scripting Tool commands to configure each instance of Access Manager 11.1.2.2.0 server to run in coexistence mode with the Oracle Access Manager 10*g* server.

1. Run the following command from the location *IAM_HOME*/common/bin to launch the WebLogic Scripting Tool (WLST):

   On UNIX:

   ./wlst.sh

   On Windows:

   wlst.cmd

2. 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 is running.

   port is the port of the Administration Server.

3. Run the following command to provide information about the user identity store of Oracle Access Manager 10*g* server and set the ObSSOCookie domain:

   ```
   setCoexistenceConfigWith10G(ldapUrl="ldap://<hostname>:<port>/" ,
   ldapPrinciple="cn=oamadmin" , ldapConfigBase="dc=com,dc=oracle,dc=us" ,
   coexCookieDomain="");
   ```

   In this command,

   ldapUrl is the LDAP host and the port of the configuration store used in Oracle Access Manager 10*g* deployment.

   ldapPrinciple is the LDAP DN of the administrator for the configuration store.

   ldapConfigBase is the LDAP search base for the configuration store of the Oracle Access Manager 10*g* deployment.

   coexCookieDomain is the Web Server or WebGate domain of 10*g* Authenticating WebGate. It is important to know the authenticating domain of the 10*g* WebGate as the ObSSOCookie set by the DCC must flow to the Oracle Access Manager 10*g* server.

   For Example:

   ```
   setLdapConfigForCoexistenceWith10G(ldapUrl="ldap://<hostname>:<port>" ,
   ldapPrinciple="cn=oamadmin", ldapPolicybase="dc=com,dc=oracle,dc=us",
   coexCookieDomain="")
   ```

   You are prompted to enter the LDAP administrator's password.

4. Enter the LDAP administrator's password.
5. Run the following command to enable the Access Manager 11.1.2.2.0 server to run in coexistence mode with Oracle Access Manager 10*g*.

   ```
   enableOamAgentCoexistWith10G()
   ```

6. Restart Access Manager 11.1.2.2.0 server.
7. Repeat these steps to configure each instance of Access Manager 11.1.2.2.0 Server to run in coexistence mode with Oracle Access Manager 10*g* Servers.

8.10 Configuring Logout Settings

WebGate 10*g* uses the `logout.html` file to clear the session. Modify the `logout.html` file, which is generated when you register `WebGate 10g-1` with the Access Manager 11.1.2.2.0 Server, to update SERVER_LOGOUTURL parameter in the file to point to the Access Manager 11.1.2.2.0 Server's logout URL. The Access Manager 11.1.2.2.0 Server, configured in coexistence mode, removes both the cookies (OAMAuthnCookie and ObSSOCookie) from the request header.

Perform the following steps to modify the `logout.html` file which is generated when you register `WebGate 10g-1` with the Access Manager 11.1.2.2.0 Server.

1. 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`.

2. 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).

After modifying the `logout.html` file, ensure that logout works at both the WebGates and the Access Manager 11.1.2.2.0 Server. To do this, complete the following steps:

- Use the following URL to initiate and verify logout from the resource WebGate (`WebGate 10g-1`):

  ```
  http://OHS-2_host:OHS-2_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`.

  `WebGate 10g-1` redirects to the Access Manager 11.1.2.2.0 Server's logout URL. Therefore, `WebGate 10g-1` forwards the request to the Access Manager 11.1.2.2.0 server. The Access Manager 11.1.2.2.0 server clears all the sessions.

8.11 Verifying the Configuration

You must verify the configuration by doing the following:

1. Login to access the resource protected by `WebGate 10g-1`.

2. Try to access the resource protected by `WebGate 10g-2` or `WebGate 11g-1`. If you have successfully configured the servers to work in coexistence mode, you should be able to access the resources protected by these WebGates without entering the user credentials again.
3. Initiate logout and verify whether you are logged out from all the WebGates by accessing a resource. To access any resource, you should be prompted to enter your user credentials again.

8.12 Disabling Coexistence Feature

After migrating all the artifacts of Oracle Access Manager 10*g* server to Access Manager 11.1.2.2.0 server, you can decommission the Oracle Access Manager 10*g* server and stop running the Access Manager 11.1.2.2.0 server in coexistence mode. For information about migrating Oracle Access Manager 10*g* artifacts, see Chapter 2, "Migrating Oracle Access Manager 10g Environments".

1. Run the following command from the location *IAM_HOME*`/common/bin` to launch the WebLogic Scripting Tool (WLST):

   On UNIX:

   `./wlst.sh`

   On Windows:

   wlst.cmd

2. Run the following WLST command on the Access Manager 11.1.2.2.0 server to stop running the Access Manager 11.1.2.2.0 server in coexistence mode with Oracle Access Manager 10*g*.

   ```
   disableOamAgentCoexistWith10G()
   ```

3. Restart the Access Manager 11.1.2.2.0 server.

8.13 Known Issue

Oracle Access Manager 10*g* servers that have a 64 bit AES key do not support Coexistence mode

In Coexistence mode, the Access Manager 11.1.2.2.0 server requires a 128-, 192-, or 256-bit AES key, which is supported by JVM. When you install Oracle Access Manager 10*g* server, a 256-bit AES key for encryption is generated by default. If you regenerate this key in the Access System Console, a 64-bit key is generated. As JVM does not support 64 bit AES key, Access Manager 11.1.2.2.0 server cannot work in coexistence mode with Oracle Access Manager 10*g* servers that have a 64 bit AES key.

The workaround for this issue is to delete the AES key from LDAP, and then regenerate a 256-bit key in Oracle Access Manager 10*g* Server.

To delete the AES key, complete the following steps:

1. Open the configuration LDAP of Oracle Access Manager 10g Server in the LDAP browser.
2. Navigate to **Oblix** > **encryptionKey** > **cookieEncryptionKey node**.
3. Right-click **cookieEncryptionKey node**, and then click **Delete**. The key is deleted.

To regenerate a 256-bit key in Oracle Access Manager 10*g* Server:

1. Restart the Oracle Access Manager 10*g* Server and identity server.

2. Click on any link on the following URL:

   `http://host:port/identity/oblix`

   The key is generated. You can see the generated key in the LDAP browser.
3. Restart Access Manager 11.1.2.2.0 server to configure the coexistence mode.

9

Coexistence of Sun OpenSSO Enterprise 8.0 with Oracle Access Management Access Manager 11.1.2.2.0

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 (11.1.2.2.0) deployments coexist, after you migrate Sun OpenSSO Enterprise 8.0 to Oracle Access Management Access Manager 11.1.2.2.0.

This chapter contains the following sections:

9.1 Coexistence Overview

During the process of migration from OpenSSO Enterprise 8.0 to Oracle Access Manager 11.1.2.2.0, you can have both OpenSSO Enterprise 8.0 and Access Manager 11.1.2.2.0 deployments coexisting, such that some applications are protected by OpenSSO Enterprise 8.0 while others are protected by Access Manager 11.1.2.2.0. 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.

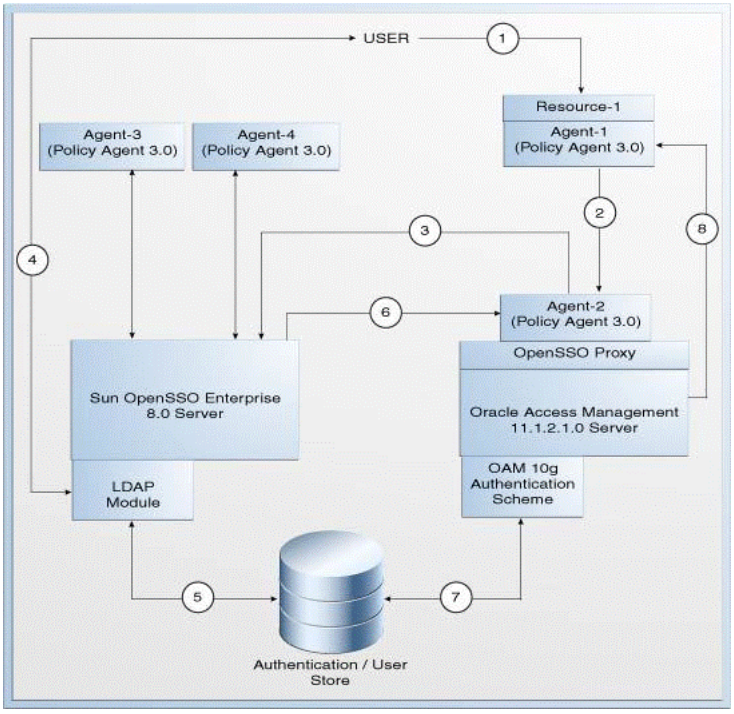
In this mode, Access Manager 11.1.2.2.0 protects the migrated applications and any new applications registered with Access Manager 11*g*; whereas OpenSSO Enterprise 8.0 continues to protect the applications that are not migrated to Access Manager 11.1.2.2.0.

In this coexistence mode, OpenSSO Enterprise 8.0 performs the authentication for all the resources protected by Access Manager 11.1.2.2.0.

9.2 Coexistence Topology

Figure 9–1 illustrates how the authentication is done by the OpenSSO Enterprise 8.0 server when a user requests to access a protected resource.

Figure 9–1 Coexistence of OpenSSO Enterprise 8.0 with Access Manager 11.1.2.2.0



The topology consists of disjoint OpenSSO Enterprise 8.0 and Access Manager 11.1.2.2.0 environments. The numbers 1-8 in the topology show the sequence in which a request flows in the coexistence environment. See Table 9–2 for the request flow.

Topology Description

- `Agent-1`: This is an OpenSSO agent (Policy Agent 3.0) registered with Access Manager 11.1.2.2.0 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 11.1.2.2.0 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 11.1.2.2.0 Server.
- `Policy-1`: This is the authentication policy created on the Access Manager 11.1.2.2.0 Server for protecting `Resource-1`. This policy is created as part of the task: Creating an Authentication Policy in Access Manager 11.1.2.2.0 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 11.1.2.2.0 Server Using Agent-2.

Table 9–2 describes the request flow. The numbers in the **Step** column correspond to the numbers in Figure 9–1.

Table 9–1 Request Flow

Step	Description
1	User requests to access `Resource-1` which is protected by `Agent-1` that communicates with the Access Manager 11.1.2.2.0 Server.
2	`Agent-1` redirects the user to the Access Manager 11.1.2.2.0 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 **OAM**10*g***AuthScheme** to assert the user from header **OAM_REMOTE_USER**.
3	The Access Manager 11.1.2.2.0 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 11.1.2.2.0 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 11.1.2.2.0 Server (….`/opensso/UI/Login/.....?goto=resource1`) after setting the header **OAM_REMOTE_USER** to the **userID** in **Session Attribute Mapping**. The Access Manager 11.1.2.2.0 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 11.1.2.2.0 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.

9.3 Task Roadmap

Table 9–2 lists the steps to configure the coexistence environment.

Table 9–2 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 11.1.2.2.0 Server using `Agent-2`.	See, Protecting the End-Point URL of Access Manager 11.1.2.2.0 Server Using Agent-2
4	Configure the data sources for Access Manager 11.1.2.2.0.	See, Configuring Data Source for Access Manager 11.1.2.2.0
5	Update the authentication module in Access Manager 11.1.2.2.0, and point the user identity store to the data source that is configured in Section 9.6.	See, Updating LDAPNoPasswordAuthModule in Access Manager 11.1.2.2.0
6	Create the profile of `Agent-1` in Access Manager 11.1.2.2.0, and install a new Policy Agent 3.0 (Agent-1) pointing to Access Manager 11.1.2.2.0 server.	See, Creating the Profile of Agent-1 in Access Manager 11.1.2.2.0
7	Create an authentication policy in Access Manager 11.1.2.2.0 server to protect `Resource-1`.	See, Creating an Authentication Policy in Access Manager 11.1.2.2.0 to Protect Resource-1

Table 9–2 (Cont.) Tasks to be Completed

Task No	Task	For More Information
8	Change the default cookie name of Access Manager 11.1.2.2.0, so that the cookie names of Access Manager 11.1.2.2.0 and OpenSSO Enterprise 8.0 are different.	See, Modifying the OpenSSO Cookie Name in Access Manager 11.1.2.2.0
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 11.1.2.2.0 Server.	See, Configuring Logout Settings
11	Verify the configuration.	See, Verifying the Configuration

9.4 Prerequisites for Coexistence

Complete the following prerequisites before you start performing the tasks described in this chapter:

- Read the system requirements and certification documents to ensure that your environment meets the minimum requirements for the products you are installing.
  - *Oracle Fusion Middleware System Requirements and Specifications*

    This document contains information related to hardware and software requirements, minimum disk space and memory requirements, and required system libraries, packages, or patches.
  - *Oracle Fusion Middleware Supported System Configurations*

    This document contains information related to supported installation types, platforms, operating systems, databases, JDKs, and third-party products.
  - For interoperability and compatibility issues that may arise when installing, refer to *Oracle Fusion Middleware Interoperability and Compatibility Guide*.

    This document contains important information regarding the ability of Oracle Fusion Middleware products to function with previous versions of other Oracle Fusion Middleware, Oracle, or third-party products. This information is applicable to both new Oracle Fusion Middleware users and existing users who are upgrading their existing environment.

    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 1.4, "Supported Starting Points for Migration and Coexistence".
- Ensure that the Sun OpenSSO Enterprise 8.0 and Oracle Access Management Access Manager 11*g* Release 2 (11.1.2.2.0) installations are complete, and the servers are running.

  If you have not installed and configured Oracle Access Management Access Manager 11*g* Release 2 (11.1.2.2.0), 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 (11.1.2.2.0), see "Installing Oracle Identity and Access Management (11.1.2.2.0)" 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 11.1.2.2.0 share the same user store.
- If OpenSSO Enterprise 8.0 and Access Manager 11.1.2.2.0 servers are running on different machines, make sure the time of these machines are synchronized.

9.5 Protecting the End-Point URL of Access Manager 11.1.2.2.0 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 11.1.2.2.0 server. Also, you must create a policy for protecting the end-point URL of the Access Manager 11.1.2.2.0 Server in OpenSSO Enterprise 8.0 Server. To do this, complete the following tasks:

1. Creating Agent-2 Profile for Access Manager 11.1.2.2.0 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 11.1.2.2.0

9.5.1 Creating Agent-2 Profile for Access Manager 11.1.2.2.0 on OpenSSO Enterprise 8.0 Server

Create `Agent-2` profile (as shown in Figure 9–1) 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**.

9.5.2 Installing Agent-2 (Policy Agent 3.0)

Install `Agent-2` (Policy Agent 3.0) in front of the Access Manager 11.1.2.2.0 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*

9.5.3 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 11.1.2.2.0 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 11.1.2.2.0 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 11.1.2.2.0 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-bundle the `oam-server.ear` file with the original `META-INF/MANIFEST.MF` file, as the `META-INF/MANIFEST.MF` file needs to be part of the command to re-package the `oam-server.ear` file. If you do not perform this step, a standard `MANIFEST.MF` file will be created and the following information will be lost:

   ```
   Manifest-Version: 1.0
   Created-By: 2010-b01 (Sun Microsystems Inc.)
   Release-Name: Oracle Access Manager 11g
   Release Version: 11.1.2.0.0
   Release-Label: NGAM_11.1.2.2.0_GENERIC_131223.0720
   Specification-Version: 11.1.2.0.0
   Implementation-Version: 11.1.2.0.0
   Weblogic-Application-Version: 11.1.2.0.0
   Extension-List: ipf
   ipf_Extension-Name: oracle.idm.ipf
   ```

   To re-bundle `oam-server.ear` file, run the following command from the location where `oam-server.ear` file was originally unzipped to before modifying the artifacts:

   ```
   jar -cvfm oam-server.ear META-INF/MANIFEST.MF
   ```

   Note: Ensure that the original `oam-server.ear` file does not exist in the upper-level directory, as it might lead to unexpected consequences when re-packaging the file with the re-bundled `oam-server.ear` file.

5. Include a jar file that contains the `com.sun.identity.agents.filter.AmAgentFilter` class to the WebLogic `CLASSPATH`.

   You can use the `agent.jar` file that was downloaded with the agents bits when you installed WebLogic J2EE Policy Agent 3.0 in Section 9.5.2, "Installing Agent-2 (Policy Agent 3.0)". The `agent.jar` file is located at *<directory_where_policy_agent_file_was_unzipped>*`/j2ee_agents/appserver_v9_agent/lib`.

   Modify the Weblogic Server's start arguments - `CLASSPATH` variable to load `agents.jar` file on the server(s) where the `oam-server.ear` file is deployed. For information about modifying the `CLASSPATH`, see "Modifying the Classpath" in the *Oracle Fusion Middleware Command Reference for Oracle WebLogic Server*.

6. Re-package the `oam-server.ear` file to include the updated `ngsso-web.war` and `openssoproxy-urlapper.war` files.

7. Redeploy the updated `oam-server.ear` file.

9.5.4 Creating Authentication Policy on OpenSSO Enterprise 8.0 Server for Access Manager 11.1.2.2.0

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 11.1.2.2.0 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 11.1.2.2.0 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**.

9.6 Configuring Data Source for Access Manager 11.1.2.2.0

Configure the data source for Access Manager 11.1.2.2.0 by completing the following steps:

1. Log in to the Oracle Access Manager 11.1.2.2.0 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.

9.7 Updating LDAPNoPasswordAuthModule in Access Manager 11.1.2.2.0

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

1. Log in to the Oracle Access Management 11.1.2.2.0 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 11.1.2.2.0 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 9.6.

9.8 Creating the Profile of Agent-1 in Access Manager 11.1.2.2.0

You must create the profile of `Agent-1` in Access Manager 11.1.2.2.0, and install a new Policy Agent 3.0 (`Agent-1`) pointing to Access Manager 11.1.2.2.0 server.

For information about creating the profile of agent in Access Manager 11.1.2.2.0, 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.

9.9 Creating an Authentication Policy in Access Manager 11.1.2.2.0 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*.

9.10 Modifying the OpenSSO Cookie Name in Access Manager 11.1.2.2.0

You must change the default cookie name of OpenSSO Cookie in Access Manager 11.1.2.2.0 server to a new name in order to avoid conflict between the cookie names of Access Manager 11.1.2.2.0 and OpenSSO Enterprise 8.0 servers. To do this, complete the following steps:

1. Stop the Access Manager 11.1.2.2.0 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 11.1.2.2.0 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 11.1.2.2.0 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 11.1.2.2.0 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 11.1.2.2.0 Server.

9.11 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 11.1.2.2.0, 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**.

9.12 Configuring Logout Settings

You must configure logout settings to have single logout across OpenSSO Enterprise 8.0 and Access Manager 11.1.2.2.0 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 11.1.2.2.0 Server

9.12.1 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 11.1.2.2.0 Server.

9.12.2 Settings to Initiate Logout from Access Manager 11.1.2.2.0 Server

To initiate logout from the Access Manager 11.1.2.2.0 Server, you must update the **Logout URL** in the respective Policy Agent 3.0 (`Agent-1`) configured with Access Manager 11.1.2.2.0 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 11.1.2.2.0 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 11.1.2.2.0 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`.

9.13 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 9–1), 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 11.1.2.2.0 Server, and observe that all the three cookies (**cookie1**, **cookie2**, and **OAM_ID** cookie) are cleared.

10

Coexistence of Sun Java System Access Manager 7.1 with Oracle Access Management Access Manager 11.1.2.2.0

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 (11.1.2.2.0) deployments coexist, after you migrate from Sun Java System Access Manager 7.1 to Access Manager 11.1.2.2.0.

This chapter contains the following sections:

10.1 Coexistence Overview

During the process of migration from Sun Java System Access Manager 7.1 to Oracle Access Manager 11.1.2.2.0, 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 11.1.2.2.0. 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.

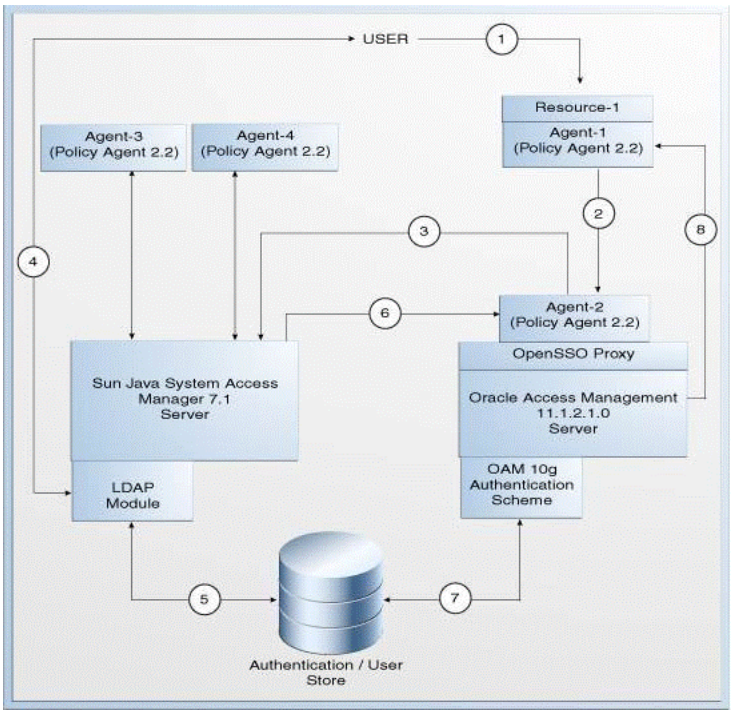
In this mode, Access Manager 11.1.2.2.0 protects the migrated applications and any new applications registered with Access Manager 11.1.2.2.0; whereas Sun Java System Access Manager 7.1 continues to protect the applications that are not migrated to Access Manager 11.1.2.2.0.

In this coexistence mode, Sun Java System Access Manager 7.1 performs the authentication for all the resources protected by Access Manager 11.1.2.2.0.

10.2 Coexistence Topology

Figure 10–1 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 10–1 Coexistence of Sun Java System Access Manager 7.1 with Access Manager 11.1.2.2.0



The topology consists of disjoint Sun Java System Access Manager 7.1 and Access Manager 11.1.2.2.0 environments. The numbers 1-8 in the topology show the sequence in which a request flows in the coexistence environment. See Table 10–1 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 11.1.2.2.0 Server. You can directly register 2.2 agents in Access Manager 11.1.2.2.0 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 11.1.2.2.0 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 11.1.2.2.0 Server.
- `Policy-1`: This is the policy created on Access Manager 11.1.2.2.0 server for protecting `Resource-1`. This policy is created as part of the task: Creating an Authentication Policy in Access Manager 11.1.2.2.0 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 11.1.2.2.0 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 10–1 describes the request flow. The numbers in the **Step** column correspond to the numbers shown in the topology in Figure 10–1.

Table 10–1 Request Flow

Step	Description
1	User requests to access `Resource-1` which is protected by `Agent-1` that communicates with the Access Manager 11.1.2.2.0 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 **OAM**10*g***AuthScheme** to assert the user from header **OAM_REMOTE_USER**.
3	The Access Manager 11.1.2.2.0 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 11.1.2.2.0 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 11.1.2.2.0 Server (….`/opensso/UI/Login/.....?goto=resource1`) after setting the header `OAM_REMOTE_USER` to the `userID` in Session Attribute Mapping. The Access Manager 11.1.2.2.0 Server invokes OAM 10g Authentication scheme (**OAM10gAUthScheme**) as per step-2 (`Policy-1`).The Access Manager 11.1.2.2.0 server asserts the user using the header `OAM_REMOTE_USER`, using the **OAM10gScheme** configured for the `Resource-1`.
8	The Access Manager 11.1.2.2.0 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.

10.3 Task Roadmap

Table 10–2 lists the steps to configure the coexistence environment.

Table 10–2 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 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 11.1.2.2.0 Server 11.1.2.2.0 by `Agent-2`.	See, Protecting Access Manager 11g Server's End Point URL by Agent-2
4	Configure the data sources for Access Manager 11.1.2.2.0.	See, Configuring Data Source for Access Manager 11.1.2.2.0
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 10.6.	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 11.1.2.2.0
7	Create an authentication policy on the Access Manager 11.1.2.2.0 Server to protect `Resource-1`.	See, Creating an Authentication Policy in Access Manager 11.1.2.2.0 to Protect Resource-1

Table 10–2 (Cont.) Tasks to be Completed

Task No	Task	For More Information
8	Change the default cookie name of Access Manager 11.1.2.2.0, 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 11.1.2.2.0
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 11.1.2.2.0 Server.	See, Configuring Logout Settings
11	Verify the configuration.	See, Verifying the Configuration

10.4 Prerequisites for Coexistence

Complete the following prerequisites before you start performing the tasks described in this chapter:

- Read the system requirements and certification documents to ensure that your environment meets the minimum requirements for the products you are installing.
  - *Oracle Fusion Middleware System Requirements and Specifications*

    This document contains information related to hardware and software requirements, minimum disk space and memory requirements, and required system libraries, packages, or patches.
  - *Oracle Fusion Middleware Supported System Configurations*

    This document contains information related to supported installation types, platforms, operating systems, databases, JDKs, and third-party products.
  - For interoperability and compatibility issues that may arise when installing, refer to *Oracle Fusion Middleware Interoperability and Compatibility Guide*.

    This document contains important information regarding the ability of Oracle Fusion Middleware products to function with previous versions of other Oracle Fusion Middleware, Oracle, or third-party products. This information is applicable to both new Oracle Fusion Middleware users and existing users who are upgrading their existing environment.

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 1.4, "Supported Starting Points for Migration and Coexistence".
- Ensure that the Sun Java System Access Manager 7.1 and Oracle Access Management Access Manager 11*g* Release 2 (11.1.2.2.0) installations are complete, and the servers are running.

  If you have not installed and configured Oracle Access Management Access Manager 11*g* Release 2 (11.1.2.2.0), 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 (11.1.2.2.0), see "Installing Oracle Identity and Access Management (11.1.2.2.0)" 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 11.1.2.2.0 share the same user store.
- If Sun Java System Access Manager 7.1 and Access Manager 11.1.2.2.0 servers are running on different machines, make sure that the time of these machines are synchronized.

10.5 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 11.1.2.2.0 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

10.5.1 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 10–1) 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**.

10.5.2 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*.

10.5.3 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 11.1.2.2.0 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 11.1.2.2.0 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 11.1.2.2.0 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.

10.5.4 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 11.1.2.2.0 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 11.1.2.2.0 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**.

10.6 Configuring Data Source for Access Manager 11.1.2.2.0

Configure the data source for Access Manager 11.1.2.2.0 by completing the following steps:

1. Log in to the Oracle Access Manager 11.1.2.2.0 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 11.1.2.2.0 console, which is the same as the bind port for the administration server

2. Go to the **Launch Pad** tab.
3. Click **User Identity Stores** under the **Configuration** section.
4. In the **User Identity Stores** tab, click the **Create** button under **OAM ID Stores**. 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.

10.7 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 10.6 as its **User Identity Store**. To do this, complete the following steps:

1. Log in to the Oracle Access Management 11.1.2.2.0 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 10.6.

10.8 Creating the Profile of Agent-1 in Access Manager 11.1.2.2.0

You must create the profile of `Agent-1` in Access Manager 11.1.2.2.0 using Remote Registration tool, and install a new Policy Agent 2.2 (`Agent-1`) pointing to Access Manager 11.1.2.2.0 server.

For information about creating the profile of `Agent-1` in Access Manager 11.1.2.2.0, 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 11.1.2.2.0 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 11.1.2.2.0.

```
<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.

10.9 Creating an Authentication Policy in Access Manager 11.1.2.2.0 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*.

10.10 Modifying the OpenSSO Cookie Name in Access Manager 11.1.2.2.0

You must change the default cookie name of the Access Manager 11.1.2.2.0 Server to a new name in order to avoid conflict between the cookie names of Access Manager 11.1.2.2.0 and Sun Java System Access Manager 7.1 servers. To do this, complete the following steps:

1. Stop the Access Manager 11.1.2.2.0 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 11.1.2.2.0 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 11.1.2.2.0 Server.

10.11 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`.

10.12 Configuring Logout Settings

You must configure logout settings to have single logout across Sun Java System Access Manager 7.1 and Access Manager 11.1.2.2.0 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

10.12.1 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 11.1.2.2.0 server.

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

To initiate logout from the Access Manager 11.1.2.2.0 server, you must update the **Logout URL** in the respective Policy Agent 2.2 (Agent-1) configured with Access Manager 11.1.2.2.0 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 11.1.2.2.0 console using the following URL:

   http://*host*:*port*/oamconsole

2. Go to the **Launch Pad** tab.
3. Click **SSO Agents** under the **Access Manager** section.
4. Click on the **OpenSSO Agents** tab.
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*

10.13 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 10–1), 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 11.1.2.2.0 Server, and observe that all the three cookies (**cookie1**, **cookie2**, and **OAM_ID** cookie) are cleared.

A

Common Migration Tasks

This appendix lists the common migration tasks that need to be performed as part of the upgrade process.

This chapter includes the following topics:

- Appendix A.1, "Stopping the Servers"
- Appendix A.2, "Starting the Servers"

A.1 Stopping the Servers

To stop the WebLogic Administration Server and the Managed Server(s), refer to the following sections:

- Stopping the Managed Server(s)
- Stopping the WebLogic Administration Server

You must stop the Managed Server(s) first, and then the WebLogic Administration Server.

A.1.1 Stopping the Managed Server(s)

To stop the Managed Server(s), do the following:

On UNIX:

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

   cd *MW_HOME*/user_projects/domains/*domain_name*/bin

2. Run the following command to stop the servers:

   ./stopManagedWebLogic.sh *managed_server_name admin_url admin_username password*

   where

   managed_server_name is the name of the Managed Server.

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

   admin_username 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 managed_server_name admin_url admin_username password
   ```

   where

   managed_server_name is the name of the Managed Server.

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

   admin_username is the username of the WebLogic Administration Server.

   password is the password of the WebLogic Administration Server.

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

A.1.2 Stopping the WebLogic Administration Server

To stop the WebLogic Administration Server, do the following:

On UNIX:

Run the following commands:

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

```
./stopWebLogic.sh
```

On Windows:

Run the following commands:

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

```
stopWebLogic.cmd
```

A.2 Starting the Servers

To start the WebLogic Administration Server and the Managed Server(s), refer to the following sections:

- Starting the WebLogic Administration Server
- Starting the Managed Server(s)

A.2.1 Starting the WebLogic Administration Server

To start the WebLogic Administration Server, do the following:

On UNIX:

Run the following commands:

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

```
./startWebLogic.sh
```

On Windows:

Run the following commands:

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

```
startWebLogic.cmd
```

A.2.2 Starting the Managed Server(s)

To start the Managed Server(s), do the following:

On UNIX:

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

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

2. Run the following command to start theManaged Servers:

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

   where

   managed_server_name is the name of the Managed Server

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

   admin_username is the username of the WebLogic Administration Server.

   password is the password of the WebLogic Administration Server.

On Windows:

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

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

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

   ```
   startManagedWebLogic.cmd managed_server_name admin_url admin_username password
   ```

   where

   managed_server_name is the name of the Managed Server.

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

   admin_username is the username of the WebLogic Administration Server.

   password is the password of the WebLogic Administration Server.

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