Oracle® Access Manager

Configuration Manager Installation and Administration Guide

10*g* (10.1.4.2.0)

E10358-01

August 2007

This manual provides Oracle Access Manager Configuration Manager installation and setup details as well as information about pushing configuration data changes from one Oracle Access Manager 10*g* (10.1.4.0.1), or Oracle COREid Release 7.0.4, deployment to another.

ORACLE®

Oracle Access Manager Configuration Manager Installation and Administration Guide, 10*g* (10.1.4.2.0)

E10358-01

Primary Author: Gail Tiberi

Contributor: Harsha Chaitanya, Sharadchandra Chavali, Shivkumar Kore, Frank Villavicencio

Contents

3 Migrating Configuration Data Changes

4 Validating Migration Success

Preface

This *Oracle Access Manager Configuration Manager Installation and Administration Guide* provides information about pushing configuration data changes from one Oracle Access Manager 10*g* (10.1.4.0.1), or Oracle COREid Release 7.0.4, deployment to another. For example, when pushing changes from a development deployment to a pre-production deployment. Included are considerations, prerequisites, and step-by-step instructions to help ensure your success.

> **Note:** Oracle COREid was previously known as Oblix NetPoint. Oracle Access Manager was previously known as Oracle COREid. Oracle COREid 7.0.4 was made available as part of Oracle Application Server 10*g* Release 2 (10.1.2). For this reason, Oracle COREid 7.0.4 manuals were branded with 10*g* Release 2 (10.1.2).

This Preface covers the following topics:

Audience

This guide targets the needs of anyone who is responsible for installing and managing Oracle Access Manager Configuration Manager. In addition, this book is helpful for anyone responsible for pushing configuration data changes from one Oracle Access Manager 10*g* (10.1.4.0.1), or Oracle COREid Release 7.0.4, deployment to another. In this guide, configuration data refers to Oracle Access Manager, or Oracle COREid, configuration data and access policy data stored in an LDAP directory.

This document assumes that you are familiar with your network architecture, your LDAP directory, as well as firewall and internet security. In addition, you need to be familiar with your existing Oracle Access Manager, or Oracle COREid, deployments.

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible, with good usability, to the disabled community. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to

facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at

http://www.oracle.com/accessibility/

Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

TTY Access to Oracle Support Services

Oracle provides dedicated Text Telephone (TTY) access to Oracle Support Services within the United States of America 24 hours a day, seven days a week. For TTY support, call 800.446.2398.

Related Documents

For more information about Oracle Access Manager Release 10*g* (10.1.4.0.1), see the following documents:

- *Oracle Access Manager Introduction*—Provides an introduction to Oracle Access Manager, a road map to Oracle Access Manager manuals, and a glossary of terms.
- *Oracle Application Server Release Notes*—Late breaking Oracle Access Manager details. The release notes are available with the platform-specific documentation. The most current version of the release notes is available on Oracle Technology Network at: http://www.oracle.com/technology/documentation.
- *Oracle Access Manager Patchset Notes Release 10.1.4 Patchset 1 (10.1.4.2.0) For All Supported Operating Systems.* It provides the system requirements and instructions needed to install or de-install the Patchset itself, a list of known issues related to the patchset, a list of the platform-specific bugs fixed in this Oracle Access Manager Patchset.
- *Oracle Access Manager List of Bugs Fixed Release 10.1.4 Patchset 1 (10.1.4.2.0)* . It supplements the Patchset notes document for this release. It provides a list of all generic (common to all operating systems) Oracle Access Manager bugs that have been fixed in this Patchset, sorted by component.
- *Oracle Access Manager Installation Guide*—Explains how to install and configure the components.
- *Oracle Access Manager Upgrade Guide*—Explains how to upgrade earlier releases to the latest major Oracle Access Manager release.
- *Oracle Access Manager Identity and Common Administration Guide*—Explains how to configure Identity System applications to display information about users, groups, and organizations; how to assign permissions to users to view and modify the data that is displayed in the Identity System applications; and how to configure

workflows that link together Identity application functions, for example, adding basic information about a user, providing additional information about the user, and approving the new user entry, into a chain of automatically performed steps. This book also describes administration functions that are common to the Identity and Access Systems, for example, directory profile configuration, password policy configuration, logging, and auditing.

- *Oracle Access Manager Access Administration Guide*—Describes how to protect resources by defining policy domains, authentication schemes, and authorization schemes; how to allow users to access multiple resources with a single login by configuring single- and multi-domain single sign-on; and how to design custom login forms. This book also describes how to set up and administer the Access System.
- *Oracle Access Manager Deployment Guide*—Provides information for people who plan and manage the environment in which Oracle Access Manager runs. This guide covers capacity planning, system tuning, failover, load balancing, caching, and migration planning.
- *Oracle Access Manager Customization Guide*—Explains how to change the appearance of Oracle Access Manager applications and how to control Oracle Access Manager by making changes to operating systems, Web servers, directory servers, directory content, or by connecting CGI files or JavaScripts to Oracle Access Manager screens. This guide also describes the Access Manager API and the authorization and authentication plug-in APIs.
- *Oracle Access Manager Developer Guide*—Explains how to access Identity System functionality programmatically using IdentityXML and WSDL, how to create custom WebGates (known as AccessGates), and how to develop plug-ins. This guide also provides information to be aware of when creating CGI files or JavaScripts for Oracle Access Manager.
- *Oracle Access Manager Integration Guide*—Explains how to set up Oracle Access Manager to run with third-party products such as BEA WebLogic, the Plumtree portal, and IBM WebSphere.
- *Oracle Access Manager Schema Description*—Provides details about the Oracle Access Manager schema.

For more information about Oracle COREid Release 7.0.4, see the following manuals:

- *Oracle COREid Access and Identity Introduction Guide*—Provides an introduction to Oracle COREid, a road map to Oracle COREid manuals, and a glossary of terms.
- *Oracle COREid Access and Identity Release Notes*—Late breaking Oracle COREid details. The release notes are available with the platform-specific documentation. The most current version of the release notes and Oracle COREid Access and Identity documentation is available on Oracle Technology Network at: `http://www.oracle.com/technology/documentation`.
- *Oracle COREid Access and Identity Installation Guide*—Explains how to install and configure the components.
- *Oracle COREid Access and Identity Upgrade Guide*—Explains how to upgrade earlier versions to Oracle COREid Release 7.0.4.
- *Oracle COREid Access and Identity Administration Guide Volume 1*—Explains how to configure Identity System applications to display information about users, groups, and organizations; how to assign permissions to users to view and modify the data that is displayed in the Identity System applications; and how to configure workflows that link together Identity application functions, for example, adding

basic information about a user, providing additional information about the user, and approving the new user entry, into a chain of automatically performed steps. This book also describes administration functions that are common to the Identity and Access Systems, for example, directory profile configuration, password policy configuration, logging, and auditing.

- *Oracle COREid Access and Identity Administration Guide Volume 2*—Describes how to protect resources by defining policy domains, authentication schemes, and authorization schemes; how to allow users to access multiple resources with a single login by configuring single- and multi-domain single sign-on; and how to design custom login forms. This book also describes how to set up and administer the Access System.
- *Oracle COREid Access and Identity Deployment Guide*—Provides information for people who plan and manage the environment in which Oracle COREid runs. This guide covers capacity planning, system tuning, failover, load balancing, caching, and migration planning.
- *Oracle COREid Access and Identity Customization Guide*—Explains how to change the appearance of Oracle COREid applications and how to control Oracle COREid by making changes to operating systems, Web servers, directory servers, directory content, or by connecting CGI files or JavaScripts to Oracle COREid screens. This guide also describes the Access Manager API and the authorization and authentication plug-in APIs.
- *Oracle COREid Access and Identity Developer Guide*—Explains how to access Identity System functionality programmatically using IdentityXML and WSDL, how to create custom WebGates (known as AccessGates), and how to develop plug-ins. This guide also provides information to be aware of when creating CGI files or JavaScripts for Oracle COREid.
- *Oracle COREid Access and Identity Integration Guide*—Explains how to set up Oracle COREid to run with third-party products such as BEA WebLogic, the Plumtree portal, and IBM WebSphere.
- *Oracle COREid Access and Identity Schema Description*—Provides details about the Oracle COREid schema.
- *Oracle Access Manager Configuration Manager Installation and Administration Guide*—Provides information about pushing configuration data changes from one Oracle Access Manager 10*g* (10.1.4.0.1), or Oracle COREid Release 7.0.4, deployment to another. Included are considerations, prerequisites, and step-by-step instructions to help ensure your success.

Conventions

The following text conventions are used in this document:

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

1

Configuration Management Overview

Oracle Access Manager Configuration Manager is a standalone application that is available as part of the Oracle Access Manager 10*g* (10.1.4.0.1) release. Oracle Access Manager Configuration Manager is a Java application that automates the process of managing and migrating Oracle Access Manager 10*g* (10.1.4.0.1), or Oracle COREid Release 7.0.4, configuration data. This chapter introduces this new application and includes the following topics:

Deployment Scenarios

It is possible to have more than one installation (**deployment**) of either **Oracle Access Manager** 10*g* (10.1.4.0.1) or Oracle **COREid** release 7.0.4. Like many customers, you might have several software deployments in various settings, including:

- A development deployment is ideally a *sandbox*-type setting where the dependency on the overall deployment is minimal
- A QA deployment is typically a smaller shared deployment used for testing
- A pre-production deployment is typically a shared deployment used for testing with a wider audience
- A production deployments is fully shared and available within your enterprise on a daily basis

You can even have multiple deployments of the same type. Deployments in your enterprise can have the same designations as those listed, or different designations.

Oracle Access Manager Configuration Manager provides automated processing to streamline your data **migration** tasks, help eliminate errors, and reduce system downtime to a minimum. Using the Configuration Manager, you can easily migrate configuration data (push a copy) from one deployment to another. For example if you have defined and tested a new password policy in your QA deployment, you can propagate the new policy to a production deployment.

About Oracle Access Manager Configuration Manager

The term **configuration management** refers to the *life-cycle management* of specific Oracle Access Manager 10*g* (10.1.4.0.1), or Oracle COREid Release 7.0.4, configuration data. Oracle Access Manager Configuration Manager enables you to automate the task of pushing configuration data changes from a specified directory in one deployment (the **source**) to an associated directory in another deployment of the same release (the **target**).

The term **configuration data** refers to product-specific Oracle Access Manager, or Oracle COREid, configuration and access policy data. This data is stored in the **`oblix` tree** of a Lightweight Directory Access Protocol (LDAP) **directory** within each Oracle Access Manager, or Oracle COREid, deployment. Oracle Access Manager migrates only **LDAP** data, not files, by connecting to the LDAP directory in each deployment. With Oracle Access Manager Configuration Manager, the term **environment** refers to an LDAP directory.

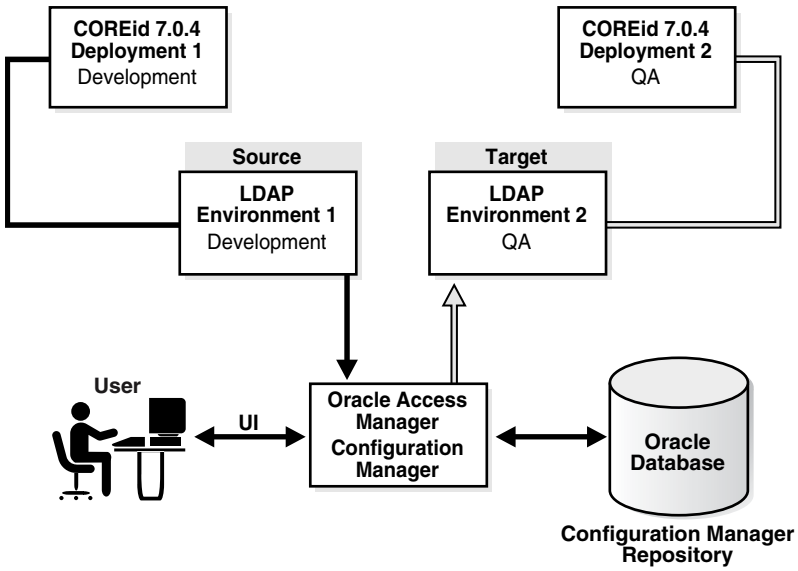
> **Note:** The process of pushing selected data to another environment is sometimes known as **horizontal data migration**, because you are copying configuration data changes for a specific release only.

When you migrate data using Oracle Access Manager Configuration Manager (also known as the Configuration Manager), you select entries in the source configuration tree to be copied to the associated target. With the Configuration Manager, you can migrate data only as follows:

- From a designated Oracle Access Manager 10*g* (10.1.4.0.1) source to an associated Oracle Access Manager 10*g* (10.1.4.0.1) target
- From a designated Oracle COREid Release 7.0.4 source to an associated Oracle COREid Release 7.0.4 target

As an example, suppose you have defined and tested a new password policy in an Oracle COREid Release 7.0.4 development deployment. Using Oracle Access Manager Configuration Manager, you can propagate the new password policy from this Oracle COREid Release 7.0.4 development deployment to your Oracle COREid Release 7.0.4 QA deployment, as shown in Figure 1–1.

Figure 1–1 Migrating Data Using Oracle Access Manager Configuration Manager



The deployments depicted in Figure 1–1 are only an example. Your deployments can differ. For example, your deployments can be Oracle Access Manager 10*g* (10.1.4.0.1). For more information, see "Deployment Support and Interoperability" on page 1-16.

Process overview: Preparing for and migrating data

1. **Repository**: After you add details about the repository to Oracle Access Manager Configuration Manager, information related to migration activities is stored in the repository.

   For more information, see "Configuration Manager Repository" on page 1-4.

2. **Environments**: After you add details about two different environments for Oracle COREid Release 7.0.4, or two different environments for Oracle Access Manager 10*g* (10.1.4.0.1), environment information is stored in the repository and you can form an association to use for migration activities.

   For more information, see "Environments" on page 1-4 and Deployment Support and Interoperability on page 1-16.

3. **Association**: After you define an association, the Configuration Manager connects to:

   - The source (the environment that contains the configuration data you want to migrate)
   - The target (the environment that you want to receive the configuration data changes)

   For more information, see "Associations" on page 1-5.

4. **Migration**: Using the Configuration Manager, you perform the automated migration processes outlined here:

   a. Create a snapshot of the target environment.

   b. Select entries in the configuration tree of the source environment.

   c. Compare details of selected entries between the source and target.

   d. Customize entries on the target, if desired.

e. Preview the data to confirm that this is what you want to migrate.

f. Migrate the selected configuration data.

The selected configuration data is copied from the source to the target. A transaction record is created in the repository that includes details about the migrated data.

See Also:

- Supported Data Types for Migration on page 1-5
- Physical Entries and Logical Objects on page 1-7
- Migration Transactions on page 1-10
- About Snapshots on page 1-14

You can choose to export selected configuration data to a Lightweight Directory Interchange Format (LDIF) file. An **LDIF file** is an ASCII format file that you can use to exchange and synchronize data between Lightweight Directory Access Protocol (LDAP) servers using an external tool. For more information, see "LDIF Files for Offline Data Importation" on page 1-10.

5. After migrating data, Oracle recommends that you test the changes in the live target deployment to validate that things are operating as expected.

   For more information about validating migration success, see Chapter 4.

Configuration Manager Repository

Oracle Access Manager Configuration Manager requires its own data store known as a **repository**. The repository must be independent of any Oracle Access Manager 10*g* (10.1.4.0.1), or Oracle COREid Release 7.0.4, deployment.

Only Oracle Database Server 10*g* Release 2 (10.2) is supported for the Oracle Access Manager Configuration Manager repository. Table 1–1 lists the information that is stored in the repository.

Table 1–1 Configuration Manager Data Stored in the Repository

Data in the Repository
Environment (directory) details
Association details
Transformation rules
Snapshots
Transaction data (logical objects migrated)
Audit details
LDIF files to import

For more information, see "Installing and Setting up the Oracle Database Repository" on page 2-6.

Environments

The term **environment** refers to an LDAP directory server that is installed and configured to operate within a specific Oracle Access Manager 10*g* (10.1.4.0.1), or Oracle COREid Release 7.0.4, deployment. The LDAP directory (environment)

includes Oracle Access Manager, or Oracle COREid, configuration data in the `oblix` tree.

Oracle Access Manager Configuration Manager does *not* require that the DIT (DN suffix) structure on each environment be exactly the same. For example, you might have configuration data in one environment with a distinguished name (DN) of `o=Oblix, ou=Config, ou=Dev, o=Root1` and another with a **configuration dn** of `o=Oblix, ou=Config, ou=QA, o=Root2`.

You add details about individual environments to Oracle Access Manager Configuration Manager. Environment details are stored in the Configuration Manager repository and are available within the Configuration Manager. For more information, see "Adding and Managing Environment Details in the Configuration Manager" on page 3-4.

After you have defined at least two environments within the Configuration Manager, you can form an association, as described next.

Associations

An **association** consists of a pair of environments that you define within the Configuration Manager. Each association includes a designated source environment from which data objects are selected, and a designated target environment to which the data is copied. For example, you can define associations to push data:

- From dvelopment to QA
- From QA to preproduction
- From preproduction to production

You can form an association between any two defined environments in the Configuration Manager. Both environments in an association are presumed to belong to deployments of the same release (either 10*g* (10.1.4.0.1) or release 7.0.4).

Any environment can be designated as either a source or a target. A single environment can be a source in one association as well as a target in another association.

You can define and use multiple associations. However, only one association is used during each migration operation. All migration history related to a specific **transaction** between the designated source and target belongs to the association.

For more information, see "Creating and Managing Associations" on page 3-12.

Caution: You cannot use Oracle Access Manager Configuration Manager to migrate data from a release 7.0.4 deployment to a release 10*g* (10.1.4.0.1) deployment nor vice versa. For more information, see "Deployment Support and Interoperability" on page 1-16.

Supported Data Types for Migration

This topic outlines the types of configuration and run-time data that you can migrate using Oracle Access Manager Configuration Manager.

Oracle Access Manager migrates only LDAP data for migration, not files. This data includes product-specific Oracle Access Manager, or Oracle COREid, configuration and access policy data for access control policies, DB profiles and instances, and other items. The data is stored in the `oblix` tree of an LDAP directory (environment) within your Oracle Access Manager, or Oracle COREid, deployments.

Table 1–2 outlines the **configuration data** types that you can migrate for the Identity System. For an overview of the Identity System, see the *Oracle Access Manager Introduction*.

Table 1–2 Identity System Configuration Data Types Supported for Migration

Migrate using Oracle Access Manager Configuration Manager	Migrate using Oracle Access Manager Configuration Manager
Password policies	Lost password policies
Administrator information	Server settings
Object class definitions	Directory options
Identity Server definitions	WebPass definitions
Master auditing policy	Global auditing policy
Substitution rights	Containment policy
Auditing policies for the: ■ User Manager ■ Group Manager ■ Organization Manager	

Table 1–3 identifies the types of Identity System run-time data that you can migrate using Oracle Access Manager Configuration Manager.

Table 1–3 Identity System Run-time Data Supported for Migration

Migrate using Oracle Access Manager Configuration Manager	Migrate using Oracle Access Manager Configuration Manager
Panels for the: ■ User Manager ■ Group Manager ■ Organization Manager	Workflow configurations: ■ User Manager workflow definition ■ Group Manager workflow definition ■ Organization Manger workflow definition
Attribute access control policies	Group Manager options
Searchbases	

Table 1–4 identifies the types of Access System configuration data that you can migrate using Oracle Access Manager Configuration Manager. For more information about the Access System, see the *Oracle Access Manager Introduction* guide.

Table 1–4 Access System Configuration Data Types Supported for Migration

Migrate using Oracle Access Manager Configuration Manager	Migrate using Oracle Access Manager Configuration Manager
Master Web resource administrators	Managed reports
Auditing policies	Master auditing policy
Access Server details	Access Server Cluster details
Authentication schemes	Authorization schemes
Host identifiers	Resource type definitions
Access client details	

Access System Run-time Data: Policy domains are the only Access System run-time data that you can migrate using Oracle Access Manager Configuration Manager. For more information about data types that can be migrated, see "Physical Entries and Logical Objects". For specific details about each of the objects and attributes, see the *Oracle Access Manager Schema Description* guide "About Preparing Customized Data for Manual Migration" on page 3-30.

As stated earlier, Oracle Access Manager Configuration Manager migrates only configuration and access policy data in the LDAP directory of an Oracle Access Manager deployment. It does not migrate any files. Also, Oracle Access Manager Configuration Manager does not automate data migration for all types of data. Customized data must be migrated from a source deployment to a target deployment manually.

Table 1–5 outlines the types of Identity System data that are not supported for migration using Oracle Access Manager Configuration Manager.

Table 1–5 Identity System Data to Migrate Manually

Identity System Data to Migrate Manually
PPP catalog (and associated called scripts/code)
Javascript
Images
Stylesheets

Table 1–6 outlines the Access System data types that are not supported for migration using Oracle Access Manager Configuration Manager.

Table 1–6 Access System Data to Migrate Manually

Access System Data To Migrate Manually
Authentication plug-in code
Authorization plug-in code

Manually migrating the data types in Table 1–5 and Table 1–6 is outside the scope of this manual. You can use other code management products that you might know about to check in, check out, and deploy the types of data in Table 1–5 and Table 1–6.

See Also:

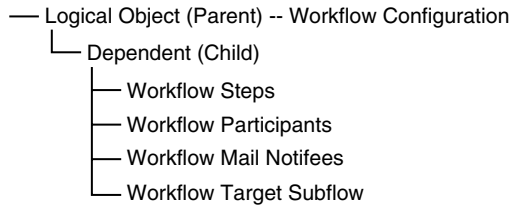
- "About Oracle Access Manager Data" on page 3-18
- "About Preparing Customized Data for Manual Migration" on page 3-30

Physical Entries and Logical Objects

In an LDAP directory, information is stored as physical entities. Many times, a group of physical entities are logically related so tightly that an individual physical entity may not make much sense with respect to the application. For example, workflow participants do not make much sense as a single entity because the participants depend on the overall workflow configuration. Such physical entities can be grouped together in Oracle Access Manager Configuration Manager under the name of one object known as a **logical object**. A logical object can also be a one-to-one mapping with a physical entity.

One logical object can have dependencies on other logical objects. For example, in Oracle Access Manager (and Oracle COREid), Workflow Configuration consists of configuration information that can be considered as a logical object with dependencies on workflow steps which in turn have dependencies on workflow participants as shown in Figure 1–2. If you choose to migrate the workflow step to the target deployment, the Configuration Manager identifies *dependent* objects such as participants, mail notifees (those who are notified by mail after the completion of a step), and the like. A dependent logical object is a *child* logical object that does not exist as a separate logical object on its own. As an example, a workflow target subflow is a dependent logical object that is not a logical object on its own.

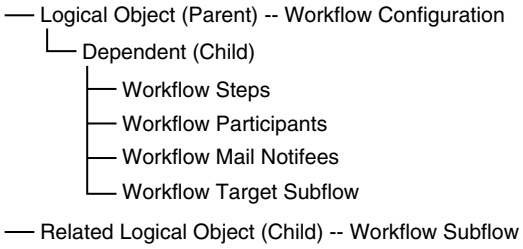
Figure 1–2 Logical Objects and Dependents



When migrating data using Oracle Access Manager Configuration Manager, all dependent logical objects are migrated along with respective parent logical objects. You cannot prevent the migration of a dependent logical object.

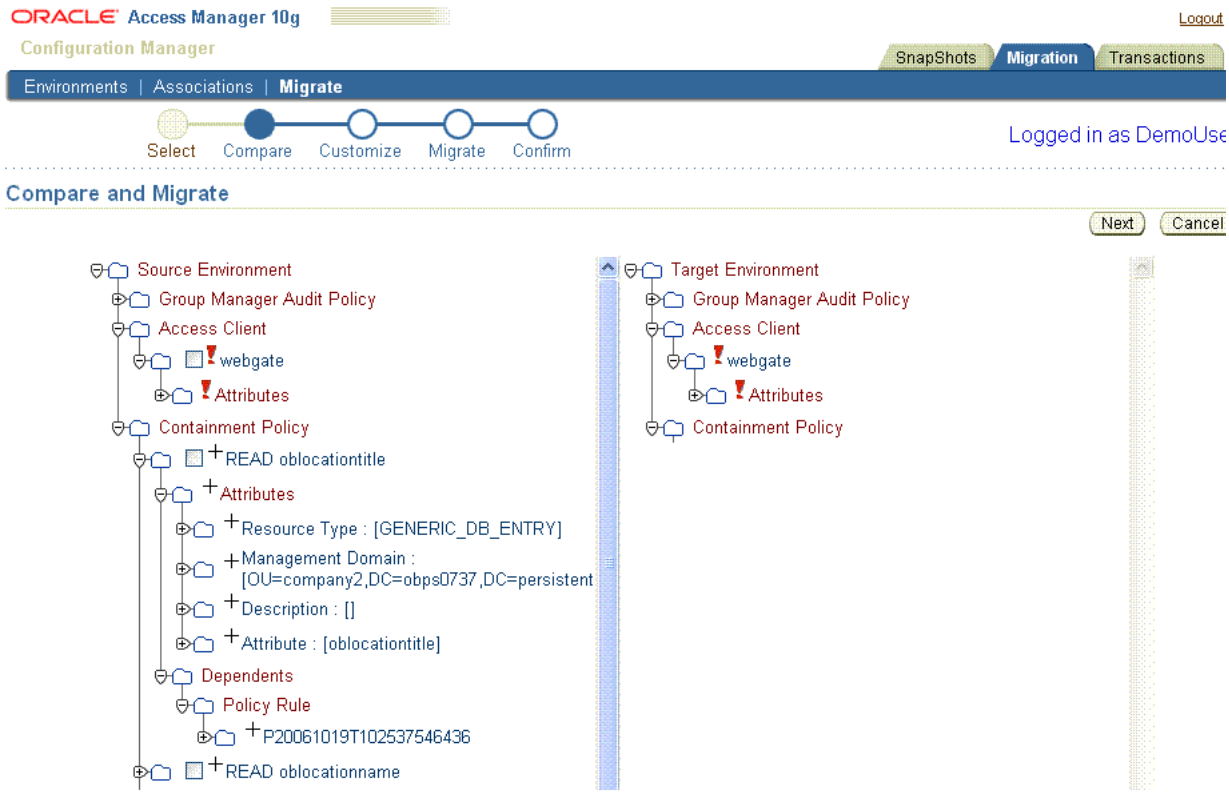
A *related* logical object is a child that exists as a separate logical object on its own. For example a lost password policy is both a logical object and a child (related) logical object of a password policy. The password policy is a logical object. Figure 1–3 illustrates a workflow definition. Here, a subflow is both a logical object and a related logical object. When migrating data using Oracle Access Manager Configuration Manager, you can either select a related logical object for migration or prevent the related logical object from being migrated by clearing the selection.

Figure 1–3 Logical Objects and Related Logical Objects



Using Oracle Access Manager Configuration Manager, you can select any number of displayed logical object types, or specific logical objects, to migrate, as described in "About Selecting Logical Objects to Migrate" on page 3-46. After selecting logical object types or specific objects, and before migrating the data, you can compare differences between the source and target in a navigation tree within the Configuration Manager as shown in Figure 1–4.

Figure 1–4 Logical Objects Presented in a Navigation Tree Structure



About Comparing and Customizing Logical Objects in Configuration Manager

On the Compare and Migrate page, you can expand items to see details about any **attribute** and dependent. Symbols beside logical object names indicate differences between the source and target before migration. For more information about the symbols, see "About Comparing Data Before Migration" on page 3-46.

Some attributes include system-specific settings and environment-specific settings such as host names, IP addresses, and domain names. You can apply changes to customize settings and attributes before, during, or after migration:

- After creating an association and before migrating data, you can create an optional transformation rule for the directory association that will be applied automatically during migration. On the Customize page, you can view logical objects as they are before the rule is applied *(Before Migration)* and as they are after the rule is applied *(After Migration)*. For more information, see "Adding and Managing Optional Transformation Rules" on page 3-31.
- During the migration, on the Customize page, you can select and customize attributes manually. After manual edits, you can view the logical object as it is before the change is applied *(Before Migration)* and as it will be after the change is applied *(After Migration)*. For more information, see "About Customizing the Target" on page 3-48.
- After migration, you can make attribute value changes using either of the following methods:
  - On the Rollback Transaction, Customize page, you can edit attributes manually much as you did if you changed attributes manually during

migration. For more information, see "Rolling Back Changes Made During a Specific Transaction" on page 5-3.

– Directly in the target Oracle Access Manager 10*g* (10.1.4.0.1), or Oracle COREid Release 7.0.4, deployment as described in the books introduced in "Related Documents" on page x.

For more information, see "About Customizing the Target" on page 3-48.

Migration Transactions

A **transaction record** is created automatically each time you migrate configuration data from a source to a target using Oracle Access Manager Configuration Manager. Each transaction record includes the entire group of logical objects and dependents, and selected related objects, that were migrated from the source to the target in an association.

A list of all transaction records is available within Oracle Access Manager Configuration Manager. You can choose a particular transaction and view the changes made during that migration. You can also select a transaction and roll back the changes to return the logical objects on the target to the state they were in before that particular migration.

Note: No transaction record is created if you choose to export data to an LDIF file.

For more information about transactions and rolling back changes, see Chapter 5.

LDIF Files for Offline Data Importation

In addition to using automated Oracle Access Manager Configuration Manager processes to migrate configuration data automatically, you can use the Configuration Manager to **export** selected configuration data to an **LDIF file**. Later, you can use the LDIF file to **import** the selected configuration data using an external tool.

Exporting to an LDIF file enables you to use Oracle Access Manager Configuration Manager with directory environments that do not provide write access to the target directory, for example, a production deployment. You can use the Export to LDIF option when:

- You want to modify the LDIF file, then import the data using an external tool.
- You want to upload the LDIF file at a scheduled time (an off-peak time, for example).
- You want to get the approval from a manager before changing the target environment.

This method employs Oracle Access Manager Configuration Manager to add environments and to form and select an association. You then select, compare, and customize logical object types on the target, and export the selections to an LDIF file using the Configuration Manager. Oracle recommends that you take a snapshot of the target environment using the Configuration Manager just before importing the data. You import the data using an external tool; this topic is outside the scope of this manual.

If you import data using the LDIF file and external tool, a transaction record is not created, because the actual migration occurs offline (outside of Oracle Access Manager Configuration Manager).

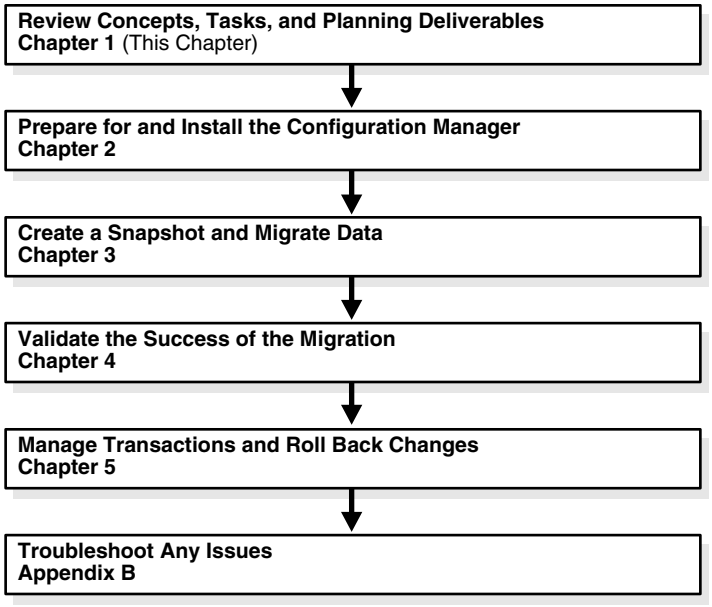
Note: You *cannot* use the Configuration Manager to import data from an LDIF file. External tools are outside the scope of this manual.

For more information, see "About Exporting Data to an LDIF File (Optional)" on page 3-50.

Migration Strategies, Methodology, and Task Overview

This section provides a very high-level introduction to the sequence of tasks that you must perform when migrating data. This is only a starting point in your planning. Figure 1–5 outlines the migration tasks that you and your team will complete when pushing configuration data changes from one Oracle Access Manager 10*g* (10.1.4.0.1), or Oracle COREid Release 7.0.4, deployment to another.

Figure 1–5 Migration Tasks



Task overview: Migrating data with Oracle Access Manager Configuration Manager

1. Review this chapter to learn about Oracle Access Manager Configuration Manager, as well as:
   - Deployment Scenarios
   - Migration Strategies, Methodology, and Task Overview
   - Data Migration Planning and Deliverables (planning worksheets are provided in Appendix A)
   - Backup and Recovery Strategies
   - Downtime Assessment and Example
   - Deployment Support and Interoperability
2. Use Chapter 2 as a guide as you install and set up required components before data migration. These preparation steps include:

a. Installing and Setting up the Oracle Database Repository for use with the Configuration Manager

b. Installing and Configuring OC4J

c. Deploying the Configuration Manager

d. Assigning Configuration Manager Administrator and User Roles in OC4J

e. Defining the Oracle Database Service Name

f. Touring the Configuration Manager

g. Adding Repository Details in the Configuration Manager

h. Ensuring the Repository is Available to the Configuration Manager

3. Use Chapter 3 as a guide to prepare and migrate configuration data from one source environment to a target environment in an Oracle Access Manager 10*g* (10.1.4.0.1), or Oracle COREid Release 7.0.4, deployment. This includes the following activities and topics:

   a. Notifying Other Administrators before and after migration

   b. Adding and Managing Environment Details in the Configuration Manager: Create, view, modify and delete directory details for existing Oracle Access Manager 10*g* (10.1.4.0.1), or Oracle COREid Release 7.0.4, deployments

   c. Creating and Managing Associations: Create new associations, view settings, enable, disable, and delete associations

   d. Adding and Managing Optional Transformation Rules that will be applied to all logical attributes in the directory association during migration

   e. Making and Managing Snapshots to make a backup copy of the `oblix` tree of the target before migrating data; you can restore the snapshot to return the target to its condition before migration, if needed

   f. Learning About Oracle Access Manager Data

   g. Migrating Data from the Source to the Target: selecting an association; selecting logical object types; comparing selected objects on the source with those on the target; customizing selected objects; previewing changes; adding a transaction description; and migrating data

      During the operation you can choose to export data to an LDIF file, then import the data offline using an external tool. For more information, see About Exporting Data to an LDIF File (Optional).

   h. Restarting Servers After Migration is required to flush their caches and update the servers with the latest configuration data from the target environment

4. Use Chapter 4 for Validating Migration Success. It includes suggestions about validating migrated data in a live target deployment. Oracle recommends that you create your own tests to validate data changes in both the source deployment before migrating data and the target deployment after migrating data.

5. Review Troubleshooting Configuration Manager Issues in Appendix B if needed.

Data Migration Planning and Deliverables

Planning and preparation are key components of any successful data migration strategy. This section discusses the planning considerations and inventory items that you and your team need to create to ensure your success:

Planning and Notifications

Before starting any data migration using Oracle Access Manager Configuration Manager, Oracle strongly recommends that you and your team become familiar with all topics suggested in Figure 1–5 on page 1-11 and the task overview that follows the figure. Oracle recommends that you schedule specific migration windows and that you notify other administrators about planned activities in any deployment for which they are responsible.

Noting Differences Between Source and Target Environments

When migrating Oracle Access Manager configuration data from one LDAP directory environment to another, be sure to note the following types of differences between the two:

- Differences in the sharing of configuration information between the Access System and the Identity System
- Differences in who is given administrative privileges, including the overall Master Administrator, Delegated Access Administrator, and Delegated Identity Administrator
- Names and implementation details of the Identity Servers
- Names and implementation details of the WebPass instances
- Names and implementation details of the Access Servers
- Names and implementation details of the WebGates, including changing what Access Server the WebGate points to
- Definitions for Host Identifiers and ipValidationExceptions
- Definitions for authentication schemes, including Challenge Redirect parameters.
- Definitions for authorization schemes
- Definitions for policy domains, including all redirect URLs defined in authentication and authorization actions
- Directory details such as computer name and port number
- Users and groups involved in policy domains

Developing Deployment Inventories

Before starting any migration activities, Oracle recommends that you take inventory of your existing Oracle Access Manager 10*g* (10.1.4.0.1), or Oracle COREid Release 7.0.4, deployments. You can gather details from existing installation (or upgrade) worksheets and records or you can gather fresh information directly from the deployment. For more information, see "Taking Inventory and Testing Operations in Existing Deployments" on page 2-4.

Developing Tests

To help ensure data correctness before migration, Oracle recommends that you develop specific tests that evaluate configuration data changes in the source deployment. After migration, you can use these same tests in the target deployment to ensure that everything is working as expected.

Deploying Oracle Access Manager Configuration Manager

Before you deploy Oracle Access Manager Configuration Manager, be sure to review the planning details in "Planning for Configuration Manager Deployment" on page 2-1.

Backup and Recovery Strategies

Oracle Access Manager Configuration Manager provides several ways to help you back up data before migration, and restore the backup after migration if needed. The following topics provide this information:

- About Snapshots
- About Transaction Records

About Snapshots

Oracle Access Manager Configuration Manager provides a SnapShot function that enables you to create a backup copy of the entire `oblix` tree in the selected environment (LDAP directory). A **snapshot** includes only the logical objects in the configuration tree. For example, workflow definitions are part of the snapshot but workflow instances are not.

If you are migrating data using the Configuration Manager, Oracle recommends that you create a snapshot of the target just before migration. If you export configuration data to an LDIF file, Oracle recommends that you create a snapshot of the target just before *importing* the LDIF file.

Using the Configuration Manager, you can **restore** a snapshot to revert all changes that were made since the snapshot was captured. This revoke changes to the logical objects in the directory and return these logical objects to the state they were in at the time the snapshot was made.

When you restore a snapshot, the entire `oblix` tree is restored to the directory. As a result of the restoration, all changes to the entire `oblix` tree are revoked. Revoked changes include both migration changes made using the Configuration Manager, as well as changes made outside the Configuration Manager.

Caution: Restoring a snapshot revokes all changes made after the snapshot was taken. Snapshot restoration returns the entire `oblix` tree in the directory to the state it was in at the time the snapshot was made.

When you restore the content of a snapshot, a new snapshot is created automatically to capture the current state of the environment. Using the new snapshot, you can undo the restoration.

For more information, see "Making and Managing Snapshots" on page 3-38.

About Transaction Records

Oracle Access Manager Configuration Manager creates a **transaction record** each time you migrate data. Each transaction record includes the entire group of logical objects, related objects, and dependents that were migrated.

> **Note:** No transaction record is created during data migration using an external tool. For example, no transaction record is created if you export data to an LDIF file using the Configuration Manager, then import the data using an external tool.

You can view details of transaction records for a selected association. In addition, you can choose a particular transaction record and:

- View the changes made during a specific migration transaction.
- Roll back the changes made during the selected transaction.

  Rolling back a transaction revokes only the changes made to logical objects during the migration transaction. During the rollback operation, a new transaction record is created.

For more information about managing transactions and rolling back changes, see Chapter 5.

Downtime Assessment and Example

You change configuration data directly for Oracle Access Manager 10*g* (10.1.4.0.1), or Oracle COREid Release 7.0.4, using the Identity (COREid) System Console or Access System Console. Your changes are automatically written to the directory directly from the deployment. In this case, appropriate entries in the server cache are flushed immediately and the server is updated with the latest configuration data. To migrate those changes to another deployment *without* the Configuration Manager, you repeat the manual process using the Identity (COREid) System Console or Access System Console. These activities are outside the scope of this manual and are described in the administration guides for your deployment as outlined in "Related Documents" on page x.

> **Note:** Manually altering data in one deployment to match data in another deployment is a time-consuming and error-prone task.

Using Oracle Access Manager Configuration Manager, you can push changes for supported logical object types from the source environment to an associated target. The automated processes are performed fairly quickly and eliminate the unintentional introduction of errors.

Oracle Access Manager Configuration Manager migrates a single logical object in approximately 100 milliseconds. Your total migration time will depend on the number of logical objects selected for migration, as well as the number of related objects and dependents. For example, it may take more time to migrate one policy domain with many host identifiers and authentication schemes than to migrate 50 or more password policies.

> **Note:** The speed and capacity of computers hosting critical components (source and target environments, OC4J, Oracle Database repository, and Oracle Access Manager Configuration Manager) will also affect the speed and duration of migration operations.

After migrating data using the Configuration Manager, you must manually restart Identity Servers and Access Servers in the target deployment to flush their caches and update the servers with the latest configuration data from the target directory. For more information, see "Restarting Servers After Migration" on page 3-55.

You can use the Configuration Manager functions to roll back a transaction. A rollback takes as long to complete as the original migration. If needed, you can restore an environment snapshot to revoke all changes made to the `oblix` tree. However, the changes you will revoke include those made during the migration as well as any made after the migration. The time it takes to restore a snapshot depends on the amount of configuration data that was backed up. For more information about managing transactions and rolling back changes, see Chapter 5.

Deployment Support and Interoperability

When you migrate data, all selected entries in the `oblix` configuration tree are copied from the source environment to the target in an association. Using Oracle Access Manager Configuration Manager you can migrate data only between:

- A designated source environment for Oracle Access Manager 10*g* (10.1.4.0.1) to an associated target within an Oracle Access Manager 10*g* (10.1.4.0.1) deployment

  For more information about Oracle Access Manager 10*g* (10.1.4.0.1), see the manuals for this release as described in "Related Documents" on page x.

- From a designated source environment for Oracle COREid Release 7.0.4 to an associated target within an Oracle COREid Release 7.0.4 deployment

  For more information about Oracle COREid Release 7.0.4, see the manuals for the release as described in "Related Documents" on page x.

> **Note:** Oracle Access Manager Configuration Manager performs automatic checks at strategic points to prohibit you from making a mistake.

You do *not* need to upgrade Oracle COREid Release 7.0.4 to Oracle Access Manager 10*g* (10.1.4.0.1). Also, Oracle Access Manager Configuration Manager does *not* perform an upgrade.

As shown in Table 1–7, both deployments represented in an association are presumed to be of the same release (either both 10*g* (10.1.4.0.1) or both release 7.0.4). Oracle Access Manager Configuration Manager operates equally well with homogeneous deployments for either release.

Table 1–7 Oracle Access Manager Configuration Manager Interoperability Matrix

From a Designated Source of Release	To a Designated Target of Release
Oracle Access Manager 10*g* (10.1.4.0.1)	Oracle Access Manager 10*g* (10.1.4.0.1)
Oracle COREid Release 7.0.4	Oracle COREid Release 7.0.4

Caution: You cannot use Oracle Access Manager Configuration Manager to migrate data from a release 7.0.4 deployment to a release 10*g* (10.1.4.0.1) deployment nor vice versa. Oracle Access Manager Configuration Manager provides checks to ensure this does not occur.

Oracle Access Manager Configuration Manager is a Java application hosted on Oracle Containers for J2EE (OC4J). Oracle Access Manager Configuration Manager deployed as an OC4J application, on one or more instances of the OC4J in either a standalone configuration or as a managed component of Oracle Application Server, will interoperate with the following additional components:

- Oracle Database repository
- Multiple environments to use as a source and target must be installed independently for Oracle Access Manager 10*g* (10.1.4.0.1) deployments
- Multiple environments to use as a source and target must be installed independently for Oracle COREid Release 7.0.4 deployments

For information about deploying and setting up the Configuration Manager, see Chapter 2.

2

Deploying and Setting Up the Configuration Manager

This chapter describes how to prepare for, deploy, and setup Oracle Access Manager Configuration Manager. The following sections are included in this chapter:

Planning for Configuration Manager Deployment

The following task overview introduces deployment and planning considerations for Oracle Access Manager Configuration Manager:

Task overview: Planning for and deploying the Configuration Manager

1. Plan for your deployment by reviewing considerations and performing required activities in following sections in this chapter:
   a. About Deploying the Configuration Manager
   b. About Planning the Number of Configuration Manager Instances Needed
   c. Deciding and Confirming Administrator Rights
   d. Taking Inventory and Testing Operations in Existing Deployments
2. Deploy Oracle Access Manager Configuration Manager as described in following sections in this chapter:
   a. Setting Up a Repository and Installing OC4J
   b. Deploying the Configuration Manager
   c. Assigning Configuration Manager Administrator and User Roles in OC4J
   d. Defining the Oracle Database Service Name

e. Adding Repository Details in the Configuration Manager

f. Ensuring the Repository is Available to the Configuration Manager

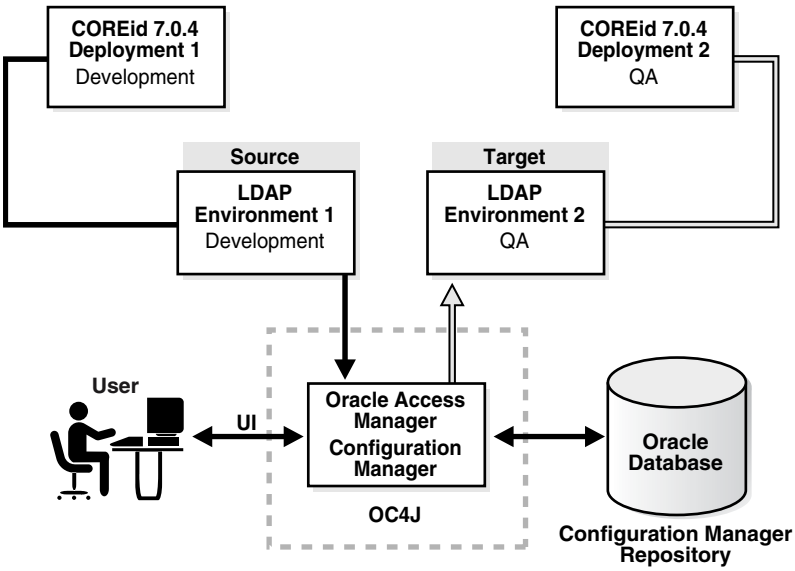
3. Add log handler and logging specific details for Oracle Access Manager Configuration Manager to the j2ee-logging.xml file as described in "Configuring Logging for Oracle Access Manager Configuration Manager" on page 2-33.

About Deploying the Configuration Manager

Oracle Access Manager Configuration Manager is a Java application hosted on OC4J. A typical Oracle Access Manager Configuration Manager deployment includes the components and applications illustrated in Figure 2–1. A description follows the figure.

Note: OC4J and Oracle Access Manager Configuration Manager must be installed together on a single platform.

Figure 2–1 Typical Oracle Access Manager Configuration Manager Installation



The sample Oracle Access Manager Configuration Manager installation depicted in Figure 2–1 shows Oracle COREid Release 7.0.4 environments. However, your deployment might instead include Oracle Access Manager 10*g* (10.1.4.0.1).

Administrators and users access Oracle Access Manager Configuration Manager through a Web browser. The Configuration Manager deployment includes:

- **Repository**: One Oracle Database 10*g* Release 2 (10.2) instance to use as the Configuration Manager repository

  For more information, see "Installing and Setting up the Oracle Database Repository" on page 2-6.

- **OC4J**: One instance of OC4J in either a standalone configuration, as depicted in Figure 2–1, or installed as a managed component of Oracle Application Server

  For more information, see "Installing and Configuring OC4J" on page 2-7.

- **The Configuration Manager**: One or more instances of Oracle Access Manager Configuration Manager deployed as an OC4J application

  OC4J and the Configuration Manager are installed together on a single platform. For more information, see "About Planning the Number of Configuration Manager Instances Needed" on page 2-3.

- **Environments**: At least two independent Oracle Access Manager 10*g* (10.1.4.0.1), or Oracle COREid Release 7.0.4, deployments and their respective LDAP directory environments (source and target LDAP directories) must be installed.

  Installing and configuring Oracle Access Manager 10*g* (10.1.4.0.1), or Oracle COREid Release 7.0.4, is outside the scope of this manual. For more information about these activities, see the books listed in "Related Documents" on page x.

  Oracle Access Manager Configuration Manager *reads* only from a single master or replica server and *writes* to only a single master LDAP directory. The installation of directory environments is outside the scope of this manual. For more information, see your directory vendor documentation.

About Planning the Number of Configuration Manager Instances Needed

Most enterprises need only one instance of Oracle Access Manager Configuration Manager, as shown in Figure 2–1 on page 2-2. If you encounter performance issues with multiple users, you may install additional Oracle Access Manager Configuration Manager instances.

> **Caution:** Multiple users migrating changes for the same logical object in the same target could create an inconsistent state on the target. Oracle recommends that users coordinate before migrating data.

One Oracle Database can serve multiple Configuration Manager instances. There are no restrictions regarding the listening port of the repository when you have multiple Configuration Manager instances. You can view and manage details in the repository from any Configuration Manager instance that is connected to that repository. For more information, see "Installing and Setting up the Oracle Database Repository" on page 2-6.

Whether you have one or more Configuration Manager instances you need only one OC4J instance. For more information, see "Installing and Configuring OC4J" on page 2-7.

Before Oracle Access Manager Configuration Manager can connect to the repository, you must define the database service name as described in "Defining the Oracle Database Service Name" on page 2-22.

Deciding and Confirming Administrator Rights

The following guidelines apply to Oracle Access Manager Configuration Manager administrators:

- Deploying the Configuration Manager requires OC4J administrator privileges. The role is created automatically during OC4J installation and setup. This account is assigned the `oc4j-administrators` role that is used to manage users and roles and to connect to the JMX MBean server.

- Managing repository details within the Configuration Manager requires `HMAdmin` privileges. The `HMAdmin` role must be defined in OC4J and assigned to any individual who will manage details and test the repository connection within the Configuration Manager.
- Configuration Manager functions, *except* managing the repository, require the `HMUser` role. The `HMUser` role must be defined in OC4J and assigned to individuals who will add environment details, create associations, make snapshots, migrate data, and manage transactions within the Configuration Manager.

> **Note:** Usesr with write privileges to an environment (directory) can perform all migration functions when they have `HMUser` privileges. Those with `HMAdmin` privileges can perform only system configuration functions in the Configuration Manager.

Information about defining administrator privileges in OC4J is described in the *Oracle Containers for J2EE Configuration and Administration Guide* 10*g* Release (10.1.3) and in "Installing and Configuring OC4J" on page 2-7.

To decide or confirm administrator rights

1. Adhere to your own corporate policies when designating administrators, choosing administrator login IDs, choosing temporary or permanent passwords, collecting and disseminating information, and so on.
2. Communicate with your team as you decide and assign administrator rights as well as user IDs and passwords for OC4J, Oracle Database, and Oracle Access Manager Configuration Manager login.

Taking Inventory and Testing Operations in Existing Deployments

This topic introduces the details that you need to collect and tests that you need to create before starting any data migration activities in a live deployment. Before starting migration activities, Oracle recommends that you perform the following activities:

- Take an inventory within Oracle Access Manager 10*g* (10.1.4.0.1), or Oracle COREid Release 7.0.4, deployments that will be involved in the migration.
- Create and perform tests in the source deployment to ensure that data changes are producing the results you expect.

Taking Inventory: Table 2–1 identifies the details that you need to collect for each installed Oracle Access Manager 10*g* (10.1.4.0.1), or Oracle COREid Release 7.0.4, deployment and where to find the worksheets where you can record the information. You can find inventory details on installation or upgrade worksheets for each deployment or you can gather fresh details from the deployment itself.

Table 2–1 Details Needed for Each Installed Deployment

Component	Specific Details Needed
Directory server instance	Worksheet for Directory Instances on page A-3
DIT and Object definitions	Worksheet for DIT and Object Definition Details on page A-4
Directory server profiles	Worksheet for Directory Server Profiles on page A-5

Table 2–1 (Cont.) Details Needed for Each Installed Deployment

Component	Specific Details Needed
Database instance profiles	Worksheet for Database Instance Profiles on page A-6
Identity Servers	Worksheet for Identity Servers on page A-7
Policy Manager details (also known as the Access Manager in Oracle COREid Release 7.0.4)	Worksheet for Policy Manager (release 7.0.4 Access Manager) Instances on page A-8
Identity Servers	Worksheet for Access Servers on page A-10
Workflows and Access Control Lists	Worksheet for Configurations on page A-11

Creating Tests: Before you migrate data to another deployment, be sure to create and perform tests to help you confirm that changes in the source are producing the desired result. In addition, you may need to reconcile the target to ensure that migrated changes operate as expected. For example if you are migrating workflow data, you want to ensure that all participants mentioned in the source environment are also present in the target. Otherwise, the workflow in the target deployment may not work properly. Oracle Access Manager Configuration Manager does *not* inform you if participants are missing in the target environment.

To take inventory, test changes in the source deployment, and reconcile the target

1. Before migration, fill in a copy of the worksheets in Appendix A as you gather and record information about existing deployments and their directories.
2. Test changes in your source deployment to ensure things are working as expected.
3. Develop appropriate tests to validate functions in the source deployment that are affected by configuration data changes to ensure that the changes produce the expected and desired result.
4. Ensure that the target includes the same participants mentioned in source environment work flows, as well as other such items that eliminate possible points of failure after migrating data.

> **Note:** After migrating data, you can use the same tests to validate migrated changes in the target deployment.

Setting Up a Repository and Installing OC4J

You must perform all activities described in the following task overview to set up the host and prepare for Oracle Access Manager Configuration Manager installation.

Task overview: Setting up a host and preparing for Configuration Manager installation includes

1. Verifying the Latest Support Requirements
2. Installing and Setting up the Oracle Database Repository
3. Installing and Configuring OC4J

Verifying the Latest Support Requirements

Before you get started with installation and setup, Oracle recommends that you verify that your computers and the selected repository are supported. You do this using the following procedure.

To verify the latest support information on MetaLink

1. Go to the Oracle MetaLink Web site at:

   `https://metalink.oracle.com`

2. Log in to Oracle MetaLink as directed.
3. Click the **Certify** tab.
4. Click **View Certifications by Product**.
5. Select the **Application Server** option and click **Submit**.
6. Choose Oracle Identity Manager and click **Submit**.
7. Click **Oracle Identity Management Certification Information 10g (10.1.4.0.1)** (html) to display the Oracle Identity Management page.
8. Click the link for **Section 6, "Oracle Access Manager Certification"** to display the certification matrix.

Installing and Setting up the Oracle Database Repository

This topic provides an overview of installing and setting up Oracle Database Server as the repository for the Configuration Manager.

You must install Oracle Database Server 10*g* Release 2 (10.2) as the repository for Oracle Access Manager Configuration Manager. The following editions are supported:

- Enterprise Edition
- Standard Edition
- Express Edition (XE)

The Configuration Manager communicates with Oracle Database in the standard way, and does *not* use Oracle Call Interface (OCI). The Configuration Manager uses the repository to store details about environments, associations, transformation rules, snapshots, transaction records, audit information, and LDIF files.

Only one repository is needed even when you plan to install multiple instances of Oracle Access Manager Configuration Manager. For more information, see "About Planning the Number of Configuration Manager Instances Needed" on page 2-3.

To install Oracle Database Server 10*g* Release 2 (10.2)

1. Verify support certifications for Oracle Database Server on MetaLink, as usual:
   a. Go to the Oracle MetaLink Web site at:

      `https://metalink.oracle.com`

   b. Log in to Oracle MetaLink as directed.
   c. Click the **Certify** tab.
   d. Click **View Certifications by Product**.
   e. Select the **Database/Server** option and click **Submit**.

f. Choose **Oracle Database -** *YourEdition* and click **Submit**.

2. Refer to the appropriate *Oracle Database Server Installation Guide* for your specific platform for installation and setup details.
3. See *Oracle Database Concepts 10g Release 2 (10.2)* for more information about Oracle Database administration and management.
4. Use the *Oracle Database Administrator's Guide 10g Release 2 (10.2)* for details about managing Oracle Database processes, tablespaces, data files, tempfiles, managing schema files, Oracle-managed files, and more.

After installing the repository, you are ready to complete activities in "Installing and Configuring OC4J". After installing OC4J, you can deploy the Configuration Manager then add details about the installed repository to the Configuration Manager.

Installing and Configuring OC4J

This topic introduces Oracle Containers for J2EE (OC4J) installation and setup.

Both OC4J and Oracle Access Manager Configuration Manager are installed together on a single platform. Before you can deploy Oracle Access Manager Configuration Manager, you must install OC4J 10g Release 3 (10.1.3).

OC4J provides a complete Java 2 Enterprise Edition (J2EE) 1.4-compliant environment. OC4J provides all containers, application programming interfaces (APIs), and services mandated by the J2EE specification.

OC4J is distributed in two configurations, both of which are supported by Oracle Access Manager Configuration Manager:

- **Standalone Configuration**: In this configuration, OC4J is installed as a single, standalone instance that is managed, started and stopped directly as a self-contained component. This OC4J configuration, also known as an *unmanaged configuration*, offers a robust J2EE-compliant container that is easy to administer. In this configuration, a single OC4J instance is installed into a single `ORACLE_HOME` (the root directory in which Oracle software is installed).

  Web communication in an OC4J standalone configuration is provided through the built-in OC4J Web server, which supports HTTP and HTTPS communications natively without the use of Oracle HTTP Server (OHS). The default Web site is defined in the default-web-site.xml file, which specifies the default HTTP listener on port 8888. You can define additional Web sites on different ports using variations of this file. See *Oracle Containers for J2EE Configuration and Administration Guide* 10*g* Release (10.1.3) for instructions on creating and managing additional Web sites in OC4J.

  For installation details, see "Installing and Configuring OC4J in a Standalone Configuration" on page 2-8.

- **Managed Configuration**: In this configuration, OC4J is installed as a component of Oracle Application Server, in a group of one or more OC4J instances within an Oracle Application Server cluster. Oracle Application Server provides support for HTTP session and stateful session Enterprise JavaBean replication and load balancing across a group of OC4J instances within a cluster topology.

  For information, see "Installing OC4J as a Managed Component of Oracle Application Server" on page 2-10.

Installing and Configuring OC4J in a Standalone Configuration

The standalone OC4J configuration consists of the following components, and requires 80 megabytes (MB) of free space:

- Oracle Containers for J2EE 10*g* Release 3 (10.1.3)
- Oracle Enterprise Manager 10*g* Application Server Control Console

  This Web-based administration application is installed by default with OC4J and is enabled immediately after installation. See details about the Oracle Enterprise Manager 10g Application Server Control Console in *Oracle Containers for J2EE Configuration and Administration Guide* 10*g* Release (10.1.3) for information about using this management interface.

The standalone OC4J distribution, which includes the Application Server Control Console, is provided as a ZIP archive. During installation you are asked to provide a port number where OC4J communicates. You may assign any port number; the default port is 8888.

Administrator Account and Role: During installation, you are asked to provide a password for the `oc4jadmin` account. This account is assigned the `oc4j-administrators` role that is used to manage users and roles and to connect to the JMX MBean server. If you do not assign a password for this account when OC4J is installed, you are prompted to set it the first time that you start OC4J. The password can later be changed through the Setup page in the Application Server Control Console. The following procedure includes details about setting the password for the `oc4jadmin` account. For more information, see details about installing standalone OC4J in *Oracle Containers for J2EE Configuration and Administration Guide* 10*g* Release (10.1.3).

Starting and Stopping OC4J: You can start an OC4J server instance in a standalone environment using the default configuration with one of the OC4J command scripts, or with the executable oc4j.jar archive. You can stop a standalone OC4J server by invoking the `-shutdown` command in the admin_client.jar or admin.jar command-line utility or by invoking an oc4j.cmd or oc4j executable script. For more information, see *Oracle Containers for J2EE Configuration and Administration Guide* 10*g* Release (10.1.3).

Default Web Site: Once installed, the standalone OC4J distribution includes a default Web site where applications can be accessed, and a Web site that allows the Application Server Control Management interface to be used. In a standalone OC4J configuration, the default Web site is configured to receive HTTP requests directly on a specific port. The default port is 8888. Alternatively, the site can be configured to receive secure HTTPS requests. The default Web sites are provided so that you can start using OC4J immediately. For more information, see *Oracle Containers for J2EE Configuration and Administration Guide* 10*g* Release (10.1.3).

The following procedure provides information that you need to install OC4J in a standalone configuration for use with Oracle Access Manager Configuration Manager. These steps are not intended to replace OC4J installation details available in the *Oracle Containers for J2EE Configuration and Administration Guide* 10*g* Release (10.1.3).

Note: The Java 2 Platform, Standard Edition (J2SE) Development Kit (JDK) release 5.0 or higher is required.

To install OC4J as a standalone server

1. Check Oracle Metalink to ensure that your host computer is compatible with this Oracle Access Manager Configuration Manager release as described in "Verifying the Latest Support Requirements" on page 2-6.
2. Before installing a standalone OC4J server, ensure that the prerequisites described in the *Oracle Containers for J2EE Configuration and Administration Guide* 10*g* Release (10.1.3) been met. This includes, among other things:
   a. On the host computer for OC4J, download and install the Java 2 Platform, Standard Edition (J2SE) Development Kit (JDK) release 5.0 or higher.
   b. After installing J2SE, ensure that the appropriate environment variables are set (or example, `JAVA_HOME`, `ORACLE_HOME`, and `J2EE_HOME`).
3. Locate and download the distribution ZIP archive for OC4J from:

   `http://www.oracle.com/technology/software/products/ias/index.html`

   ```
   For Development:
        Oracle Containers for J2EE (OC4J) 10g Release 3 (10.1.3.1.0)
   ```

4. Install the standalone OC4J distribution using instructions in the *Oracle Containers for J2EE Configuration and Administration Guide* 10*g* Release (10.1.3).

   See the instructions for extracting the oc4j_extended.zip file into the directory that will serve as the installed directory for OC4J (also known as `ORACLE_HOME`) with the archive utility of your choice.

   The installer automatically creates the required directory structure for you. You can start an OC4J server instance in a standalone environment using the default configuration with one of the OC4J command scripts or the executable oc4j.jar archive. For more information about starting and stopping OC4j, see *Oracle Containers for J2EE Configuration and Administration Guide* 10*g* Release (10.1.3).
5. Set a password for the Administrator account for OC4J the first time that you start OC4J is started (the user name for this account is set to `oc4jadmin` by default).

   Note: You can change the password for this account. For more information, see the information on tools for administering OC4J in *Oracle Containers for J2EE Configuration and Administration Guide* 10*g* Release (10.1.3).

6. Ensure that the installation is a success by entering the URL to the home page for OC4J and then login as the `oc4jadmin`. For example:

   `http://`*`hostname:port`*`/em/console`

   In the sample URL, *hostname* refers to computer that hosts OC4j standalone configuration; *port* refers to the HTTP port number on which OC4j host listens; and em/console connects to the OC4j console.
7. Proceed as follows:
   - **Installation Successful** (perform activities described in the following topics):
     - Deploying the Configuration Manager using the Enterprise Manager browser console

  - Assigning Configuration Manager Administrator and User Roles in OC4J to ensure that users can log in to Oracle Access Manager Configuration Manager after deployment

- **Installation Not Successful**: See troubleshooting tips in *Oracle Containers for J2EE Configuration and Administration Guide* 10*g* Release (10.1.3).

Installing OC4J as a Managed Component of Oracle Application Server

When installing OC4J as a managed component of Oracle Application Server you use advanced installation steps for the J2EE Server configuration. This configuration requires 570 M.B of free space.

In a J2EE Server configuration, the following components are installed:

- Oracle Containers for J2EE (OC4J) 10g (10.1.3.1.0) in one or more instances in one or more groups

  This component provides a complete Java 2 Enterprise Edition (J2EE) environment for developing Java applications.

- Oracle Enterprise Manager 10g Application Server Control Console (used for Web-based management of Oracle Application Server)

- Oracle HTTP Server 1.3, which provides front-end Web communication and load-balancing functionality is included with this installation

- Oracle Process Manager and Notification Server (OPMN), which includes the Oracle Notification Server (ONS)

  OPMN provides process control and monitoring for Oracle Application Server instances and their components. ONS is installed by default on every Oracle Application Server host. In a managed environment, you must use OPMN to start and stop all components, including OC4J and Oracle HTTP Server communications between components. See the section on starting OC4J in an Oracle Application Server environment in the *Oracle Containers for J2EE Configuration and Administration Guide* 10*g* Release (10.1.3) for details.

  OC4J runtime options and system properties can be manually set in the OPMN configuration file, opmn.xml. See details on the run-time configuration in the *Oracle Containers for J2EE Configuration and Administration Guide* 10*g* Release (10.1.3) for details.

Oracle Application Server provides support for HTTP session and stateful session Enterprise JavaBean replication and load balancing across a group of OC4J instances within a **cluster topology**. For details about cluster technology and application clustering in OC4J, see the *Oracle Containers for J2EE Configuration and Administration Guide* 10*g* Release (10.1.3).

In an Oracle Application Server clustered environment, a single Application Server Control Console can be used to manage all OC4J instances in a cluster. For more information, see the section about the Oracle Enterprise Manager 10g Application Server Control Console and tools for administering OC4J in the *Oracle Containers for J2EE Configuration and Administration Guide* 10*g* Release (10.1.3).

Installation of the various managed components is accomplished using the Oracle Universal Installer. OPMN must be installed in every `ORACLE_HOME` directory to enable monitoring of each installed component. The Oracle Universal Installer provides a number of installation options:

- Integrated Web Server, J2EE Server, and Process Management

In this configuration, all components are installed into a single ORACLE_HOME directory, including OC4J, Oracle HTTP Server, and OPMN. Multiple OC4J instances can be created within this ORACLE_HOME directory. Multiple host computers, each hosting one or more OC4J instances, can be included in an Oracle Application Server cluster.

- J2EE Server and Process Management

  This installation includes OC4J and OPMN. It can be utilized as a standalone OPMN-managed OC4J instance for development or testing purposes, or can be included within an Oracle Application Server cluster.

- Web Server and Process Management

  This installation includes only Oracle HTTP Server and OPMN. It can be used as a standalone Oracle HTTP Server instance, typically serving as the front-end Web listener for an Oracle Application Server cluster.

The following procedure provides information you need to install OC4J as a managed component for use with Oracle Access Manager Configuration Manager. These steps are not intended to replace OC4J installation details available in the *Oracle Application Server Installation Guide*.

To install Oracle Application Server J2EE Server configuration

1. Enter Oracle Metalink and ensure that your host computer is compatible with this Oracle Access Manager Configuration Manager release, as described in "Verifying the Latest Support Requirements" on page 2-6:
2. Perform activities as described for J2EE Server installation in the *Oracle Application Server Installation Guide* as follows:
   a. Verify requirements.
   b. Review the discussion about things you should know before starting the installation.
   c. Review topics about advanced installation of the J2EE Server.
3. Access the Oracle Enterprise Manager 10g Application Server Control Console using the following URL:

   ```
   http://hostname:port/em/console
   ```

   where *hostname* refers to computer that hosts Oracle Enterprise Manager 10g Application Server Control Console; *port* refers to the HTTP port number on which host listens; and em/console connects to the console.
4. Proceed as follows:
   - **Installation Successful** (perform the following activities in the order specified):
     - Deploying the Configuration Manager using the Enterprise Manager browser console.
     - Assigning Configuration Manager Administrator and User Roles in OC4J ensures that users can log in to Oracle Access Manager Configuration Manager after deployment.
   - **Installation Not Successful**: See troubleshooting tips in the *Oracle Application Server Installation Guide*.

Deploying the Configuration Manager

This section explains how to deploy Oracle Access Manager Configuration Manager as an OC4J application. Any Web server supported by OC4J is supported for the Configuration Manager. No Microsoft certification is available nor expected.

The Oracle Access Manager Configuration Manager application is distributed as a .war file that can be deployed using OC4J. The .war file requires 7.77 MB of free disk space.

The following procedure describes how to deploy and test the Configuration Manager. For details about starting and stopping OC4j, see the *Oracle Containers for J2EE Configuration and Administration Guide* 10*g* Release (10.1.3).

Check Table 2–2 to confirm that prerequisites have been completed before starting the following procedure.

Table 2–2 Deployment Prerequisites

Confirm	Prerequisite Tasks	Look in
	Install the Oracle Database Repository	Installing and Setting up the Oracle Database Repository on page 2-6
	Install OC4J	Installing and Configuring OC4J on page 2-7

To deploy the Configuration Manager using OC4J

1. Go to the home page for OC4J, if you have not already done so, then login as the `oc4jadmin`. For example:

   ```
   http://hostname:port/em/console
   ```

   In the sample URL, *hostname* refers to computer that hosts OC4j standalone configuration; *port* refers to the HTTP port number on which OC4j host listens; and em/console connects to the OC4j console.

2. On the home page for OC4J, click the Applications tab. For example:

   Applications

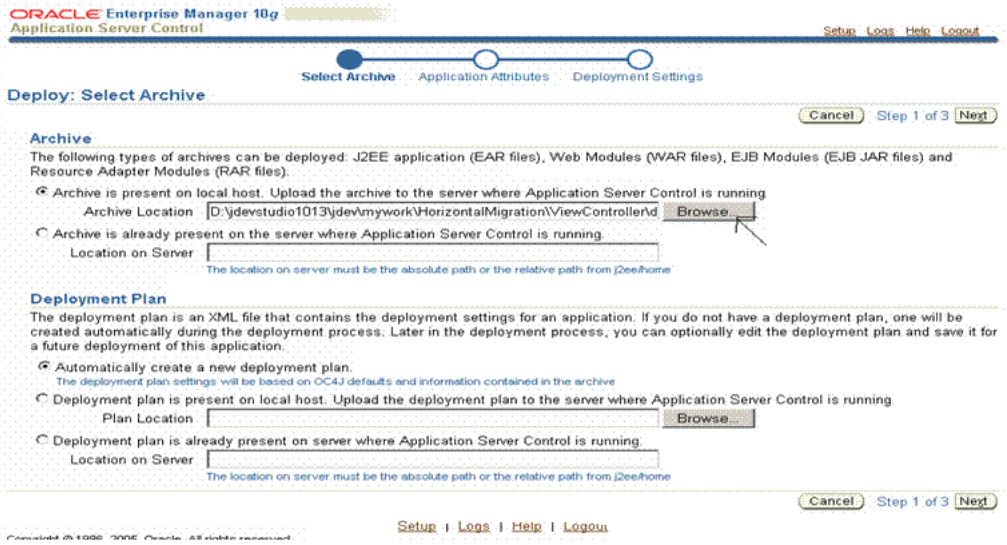
3. On the Applications page, click the Deploy button:

   Deploy

   The Select Archive page appears.

4. Fill in the path to the Oracle Access Manager Configuration Manager .war file archive using the Browse button, then click the Next button as shown in Figure 2–2.

Figure 2–2 Select Archive Page



The Application Attributes page appears.

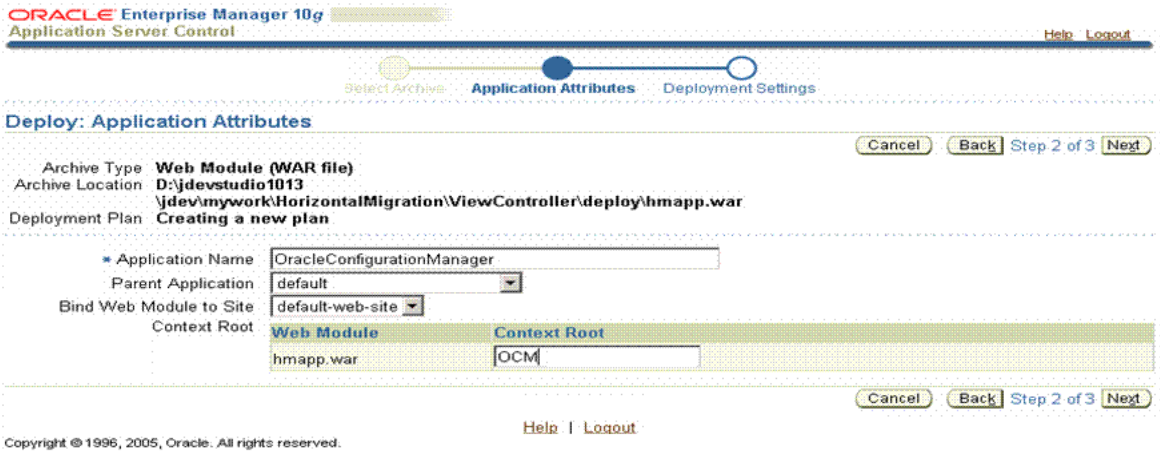
5. On the Application Attributes page, specify the values in Table 2–3 for the Configuration Manager Application Attributes, then click the Next button and compare your page with the one in Figure 2–3.

Table 2–3 Oracle Access Manager Configuration Manager Application Attribute Values

Configuration Manager Application Attributes	Values
Application Name	OracleConfigurationManger
Parent Application	default
Bind Web Module to Site	Default-web-site
Web Module Context Root	OCM

When you finish, the Application Attributes page should look something like the one in Figure 2–3.

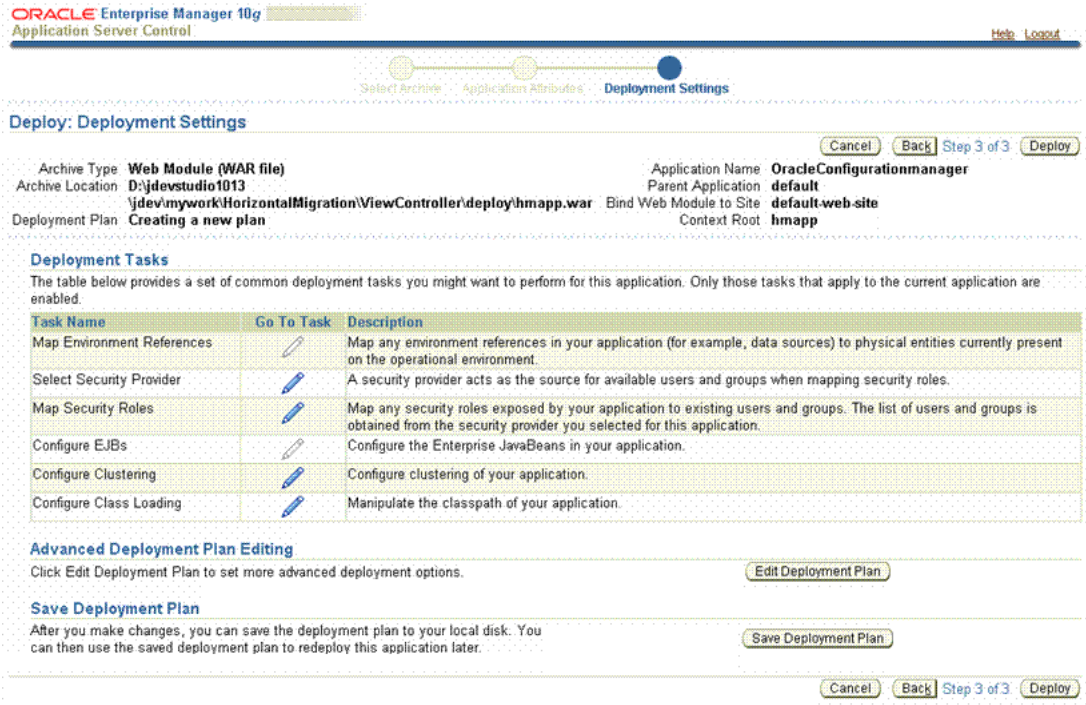
Figure 2–3 Application Attributes



When you click Next button, the Deployment Settings page appears.

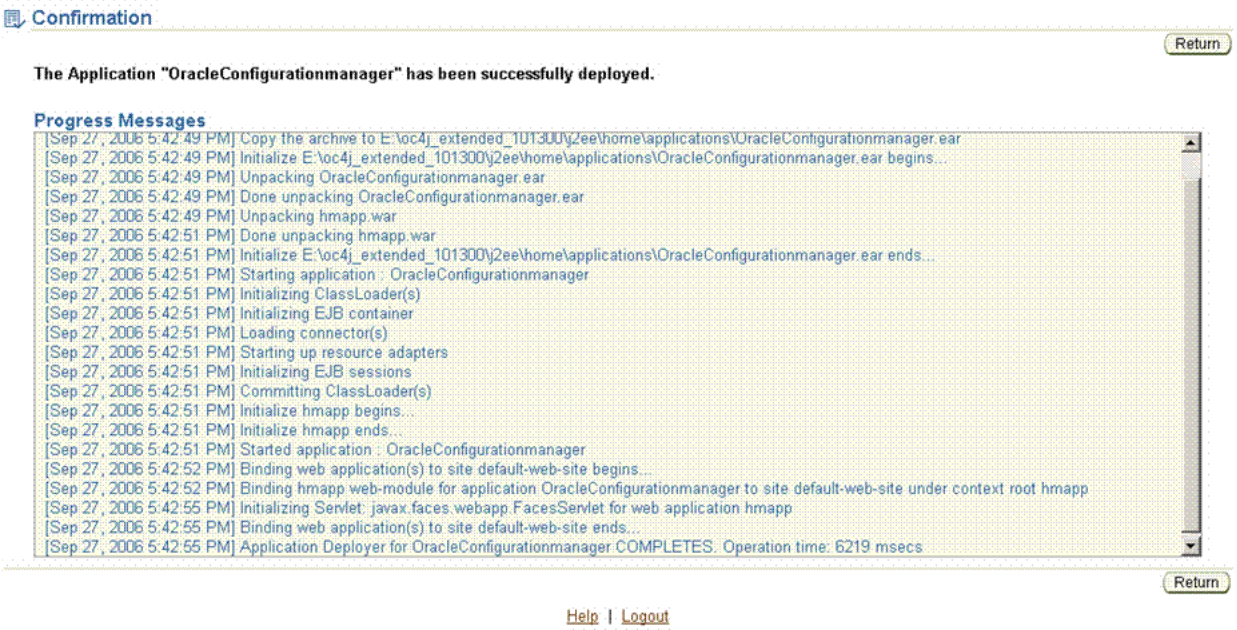
6. On the Deployment Settings page, click the Deploy button as shown in Figure 2–4 to deploy Oracle Access Manager Configuration Manager.

Figure 2–4 Deployment Settings Page



7. View the confirmation message that appears, as shown in Figure 2–5.

Figure 2–5 Confirmation Page

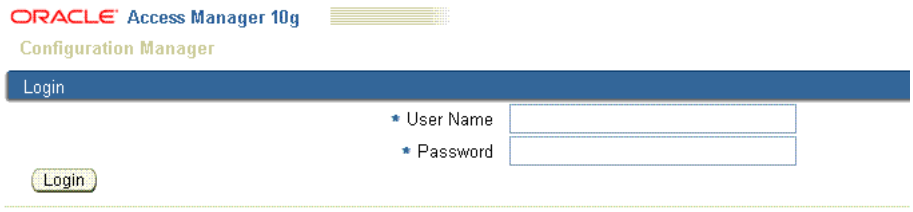


8. On the Confirmation page, click the Return button in the lower-right corner to return to the OC4J home page.
9. Test the deployment to ensure it is successful by entering the URL to the Configuration Manager home page in a browser window. For example:

   ```
   https://hostname:port/ocm/faces/index.jsp
   ```

   In the sample URL, *hostname* refers to computer that hosts the Configuration Manager; *port* refers to the HTTP port number on which the Configuration Manager host listens; /ocm refers to Web Module Context Root specified on the Application Attributes page while deploying the Oracle Access Manager Configuration Manager application; and faces/index.jsp connects to the Configuration Manager application's Login page.

   The Configuration Manager Login page should appear, as shown here.



10. Proceed as follows:
    - **Deployment Successful:** Perform activities in the following order:
      - **Logging In**: Enter the login name and password that were defined for your use with the Configuration Manager, then click the Login button. For more information, see "Assigning Configuration Manager Administrator and User Roles in OC4J" on page 2-16.

  - **Touring the Configuration Manager**: Acquaint yourself with available functions and the user interface.
  - **Adding Repository Details in the Configuration Manager**: Define the repository to be used by the Configuration Manager if you have the `HMAdmin` role assigned.

- **Deployment Not Successful**: If the Configuration Manager Login page does *not* appear, see troubleshooting tips related to deploying an application in the *Oracle Containers for J2EE Configuration and Administration Guide*.

Assigning Configuration Manager Administrator and User Roles in OC4J

The procedure in this section guides as you create then assign the administrator roles needed for Oracle Access Manager Configuration Manager.

Oracle Access Manager Configuration Manager requires only OC4J for security. Within OC4J, the Configuration Manager application requires two security roles that provide specific privileges for the Configuration Manager. Only users assigned with the following roles can perform tasks in Oracle Access Manager Configuration Manager:

- **`HMAdmin`**: This role enables you to perform *only* System Configuration functions for the repository within Oracle Access Manager Configuration Manager. To perform all other Configuration Manager activities, individuals must be assigned the `HMUser` role.
- **`HMUser`**: This role enables you to perform all Configuration Manager functions *except* System Configuration functions. A user with write privileges to an environment (directory) can perform all migration functions when they have `HMUser` privileges: add environment details, make associations and add transformation rules, take snapshots, migrate data, and manage transactions.

The `HMAdmin` and `HMUser` roles that you create in OC4J will *not* inherit any existing OC4J roles. Nor are RMI Login Permission or administration permission granted when you create the `HMAdmin` and `HMUser` role.

During Configuration Manager deployment using OC4J, you defined a specific application name for Oracle Access Manager Configuration Manager. In the following procedure, you will create the roles within OC4J that are required for administrators and users of Oracle Access Manager Configuration Manager, then assign those roles to specific users that you define within OC4J.

Check Table 2–4 to confirm that prerequisites have been completed before starting the following procedure.

Table 2–4 Assigning Configuration Manager Roles in OC4J Prerequisites

Confirm	Prerequisite Tasks	Look in
	Deploy the Configuration Manager	Deploying the Configuration Manager on page 2-12

To create and assign HMAdmin and HMUser roles in OC4J

1. Go to the home page for OC4J and login as the `oc4jadmin`. For example:

   ```
   http://hostname:port/em/console
   ```

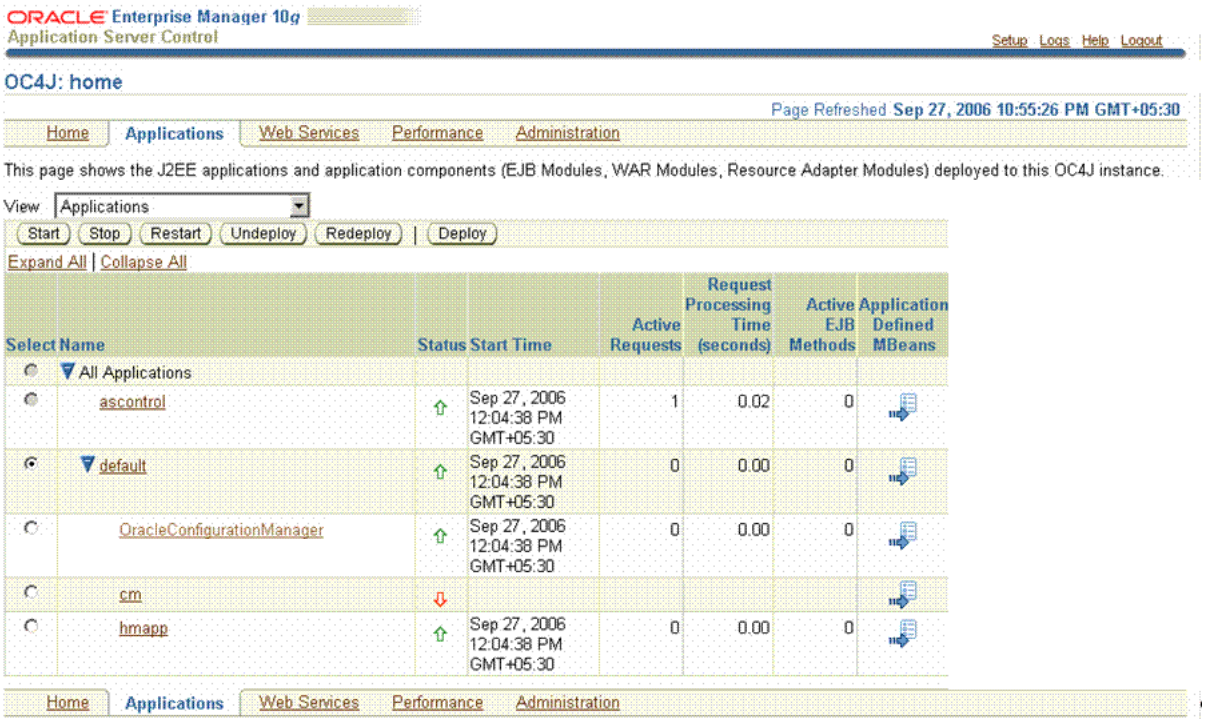
   In the sample URL, *hostname* refers to computer that hosts OC4j standalone configuration; *port* refers to the HTTP port number on which OC4j host listens; and em/console connects to the OC4J console.

2. On the home page for OC4J click the Applications tab, then locate and click the link you defined for Oracle Access Manager Configuration Manager as shown in Figure 2–6. For example:

   Applications

   OracleConfigurationManger

Figure 2–6 OC4J Applications Tab



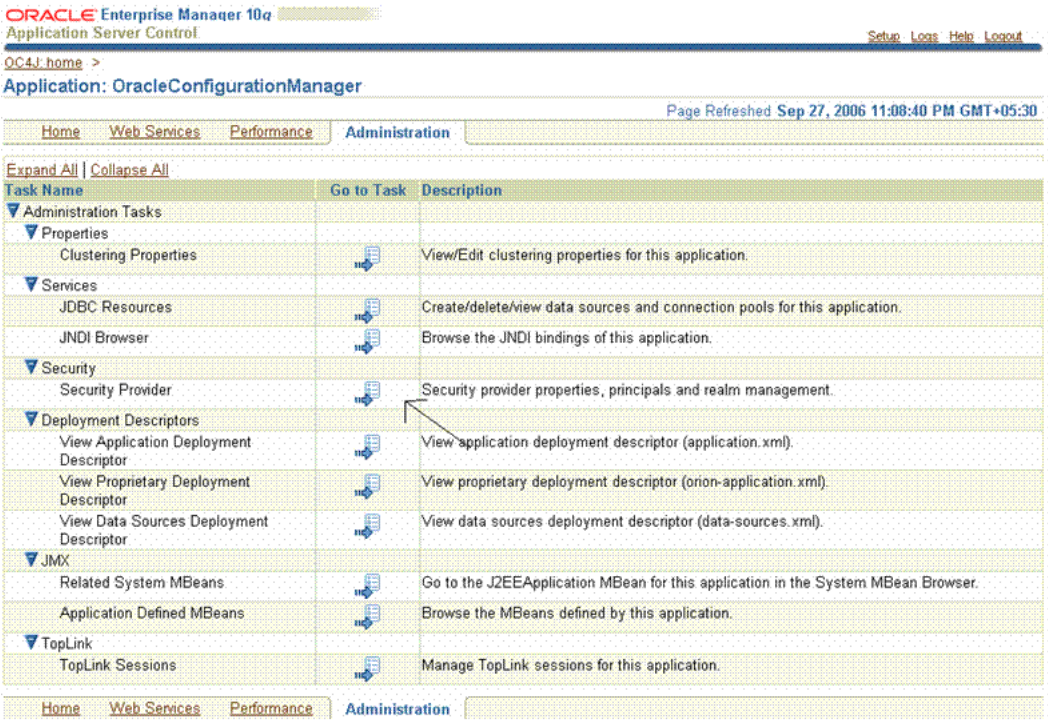
   The Applications tab for Oracle Access Manager Configuration Manager opens.

3. Click the Administration tab to display the page for Oracle Access Manager Configuration Manager. For example:

   Administration

4. On the Administration tab, click the Security Provider icon in the Go To Task column, as shown in Figure 2–7.

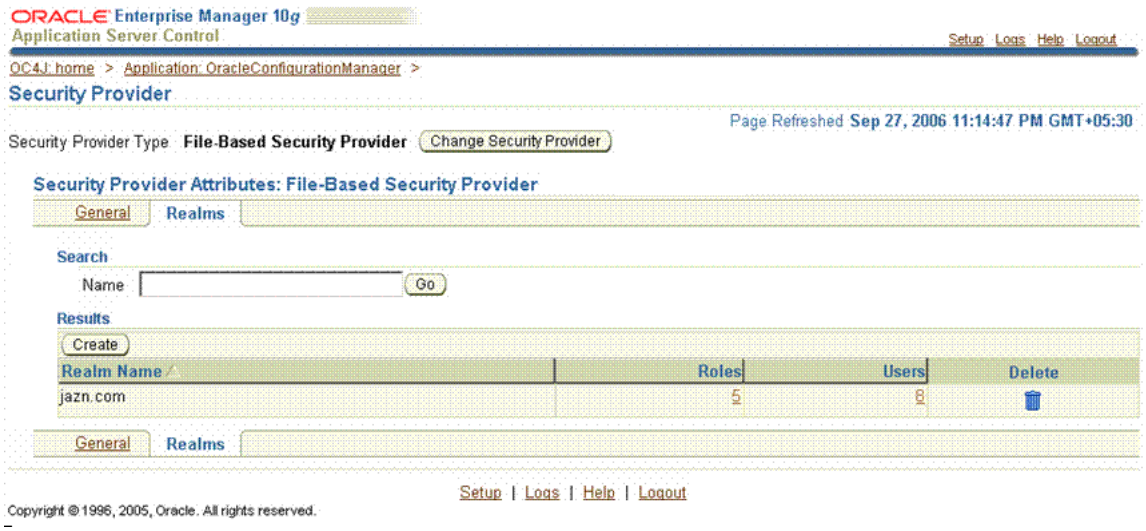
Figure 2–7 Administration Tab for Oracle Access Manager Configuration Manager



The Security Provider page appears.

5. On the Security Provider page, click the Realms tab.
6. Perform the following steps to create the `HMAdmin` and `HMUser` roles for Oracle Access Manager Configuration Manager as follows:
   a. On the Realms subtab, locate and click the link (in the Roles column) that is associated with the Realm Name as shown in Figure 2–8.

Figure 2–8 Realms Subtab: Realm Name, Roles, and Users

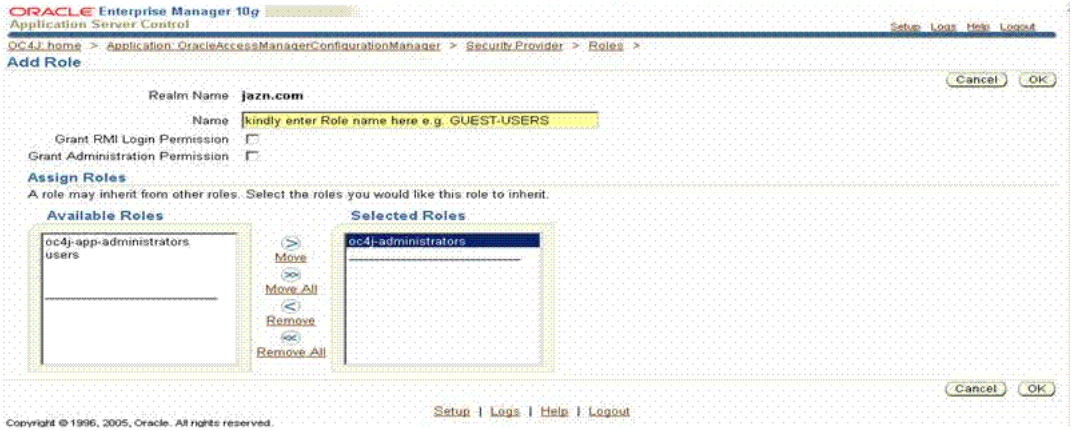


The Roles page appears and includes a Create button.

b. On the Roles page, click the Create button to display the Add Role page.

The Add Role page appears as shown in Figure 2–9.

Figure 2–9 Add Role Page



c. On the Add Role page, enter the following details for the `HMAdmin` role, then click OK:

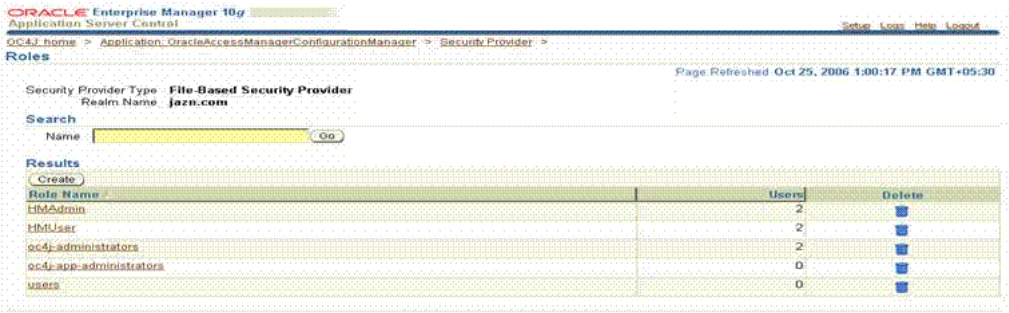
- **Name**: `HMAdmin`
- **Grant RMI Login Permission**: Leave blank.
- **Grant Administration Permission**: Leave blank.
- **Assign Roles**: Ignore; there are no roles to be inherited by HMAdmin.
- **OK**: Click the OK button when you finish to establish the `HMAdmin` role.

d. On the Add Role page, create the `HMUser` role using the following information as a guide:

- **Name**: `HMUser`
- **Grant RMI Login Permission**: Leave blank.
- **Grant Administration Permission**: Leave blank.
- **Assign Roles**: Ignore; there are no roles to be inherited by HMUser.
- **OK**: Click the OK button when you finish to establish the `HMUser` role.

Your Roles page should look something like the one in Figure 2–10.

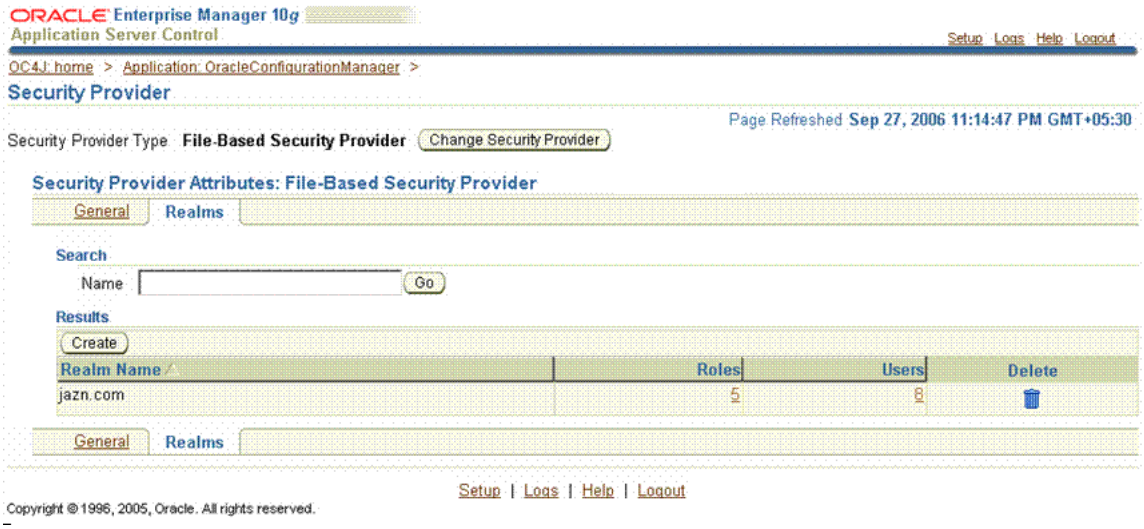
Figure 2–10 Roles Page Includes HMAdmin and HMUser



7. Add users, and assign to the Configuration Manager application the administrator or user roles that you just created, by performing the following activities:

   a. On the Realms subtab, locate and click the link in the Users column associated with the Realm Name as shown in Figure 2–11.

Figure 2–11 Realms Subtab with Users Link



   b. On the Users page, click the Create button under the Results label. For example:

      Create

   c. On the Add User Page add the requested details, then click OK as shown in Figure 2–12. For example:

      – **Username**: Enter the userid for logging in to the Configuration Manager.

      – **Password/Confirm Password**: Enter the password for this user; then confirm the password by entering it a second time.

      – **Assign Roles**: From the Available Roles list, select the desired role for this user then click the Move arrow to add these to the Selected Roles list. For example:

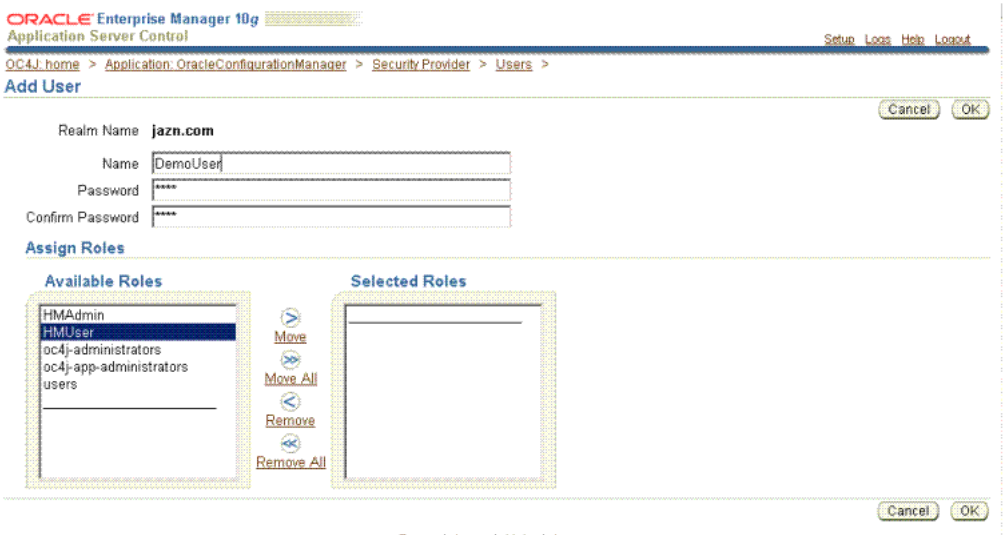
        `HMAdmin`

        or

`HMUser`

Note: A single user may be assigned both `HMAdmin` and `HMUser` roles.

Figure 2–12 Add User Page

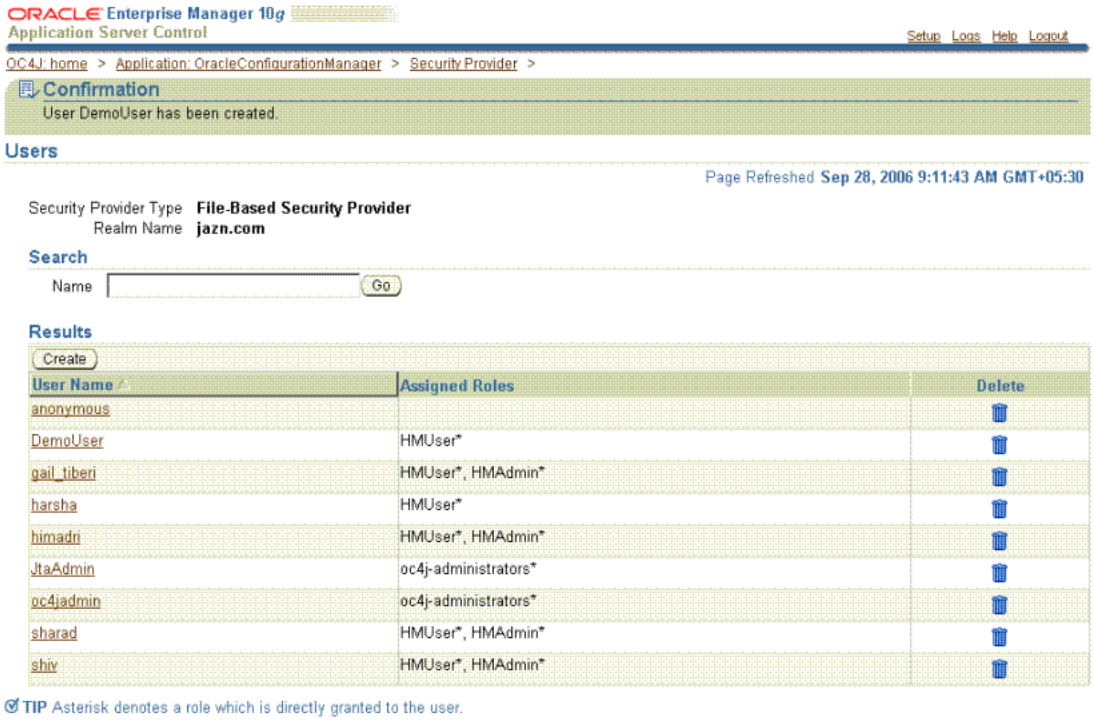


– Click **OK** to complete the operation.

  A Confirmation page appears where you can verify information for this new user.

d. On the Confirmation page, review the User Name and Roles as shown in Figure 2–13 to ensure that everything is accurate.

Figure 2–13 Confirmation Page with User Name and Roles



8. Repeat step 7 to add other Oracle Access Manager Configuration Manager administrators and users, if needed.
9. Click Logout when you finish to leave OC4J.

   With at least one Oracle Access Manager Configuration Manager administrator assigned, repository details may be added in the Configuration Manager.
10. After the roles and users have been created, restart the Oracle Access Manager Configuration Manager application and then proceed to "Defining the Oracle Database Service Name".

Defining the Oracle Database Service Name

To connect to the Oracle Database repository, Oracle Access Manager Configuration Manager requires the database service mame. To specify the database service name, you must enter the DB.Oracle.ServiceName parameter in the Oracle Access Manager Configuration Manager WEB-INF/config/db.properties file, as described in the following procedure. Typically, the database administrator has this information.

To define the database service name

1. After deploying Oracle Access Manager Configuration Manager using OC4J, locate the file:

   OC4J-HOME/j2ee/home/applications/*context-name*/*deployed-war-name*/WEB-INF/config/db.properties

   where *OC4J-HOME* is the installation directory of your OC4J instance; *context-name* refers to Web Module Context Root specified on the Application Attributes page while deploying the Oracle Access Manager Configuration

Manager using OC4J; *deployed-war-name* is the name of the Oracle Access Manager Configuration Manager war file that you deployed.

2. In the db.properties file, locate the following parameter:

   DB.Oracle.ServiceName=XE

3. Replace "XE" with the appropriate Database Service Name, if needed. For example:

   DB.Oracle.ServiceName=**EE**

4. Save the file.

5. Restart Oracle Access Manager Configuration Manager.

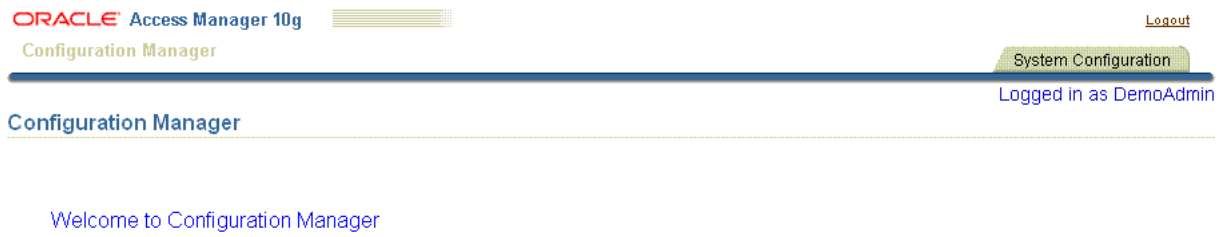
Touring the Configuration Manager

This section provides a quick tour to orient you to Oracle Access Manager Configuration Manager.

If you log in to Oracle Access Manager Configuration Manager as a user with only `HMAdmin` privileges, you see *only* the System Configuration tab. If you log in as a user with `HMUser` privileges, you see all function tabs *except* System Configuration. If you are assigned *both* roles, all tabs are available. For more information see, "Assigning Configuration Manager Administrator and User Roles in OC4J".

After logging in to Oracle Access Manager Configuration Manager, a Welcome page appears as shown in Figure 2–14. As with other Oracle Web-based applications. Function tabs are provided across the top of the page with corresponding links at the bottom of the page.

Figure 2–14 Oracle Access Manager Configuration Manager Welcome Page



To access the Configuration Manager

1. Go the Configuration Manager home page. For example:

   ```
   https://hostname:port/ocm/faces/index.jsp
   ```

   In the sample URL, *hostname* refers to computer that hosts the Configuration Manager; *port* refers to the HTTP port number on which the Configuration Manager host listens; /ocm refers to Web Module Context Root specified on the Application Attributes page while deploying the Oracle Access Manager Configuration Manager application; and faces/index.jsp connects to the Configuration Manager application's Login page.

   The Login page appears.

2. Log in as an individual with either `HMUser` or `HMAdmin` privileges, depending upon the activities you intend to perform. For example:

   HMUser_Name
   Passwword

3. As you proceed with the tour, refer to the following topics:
   - Logout Link
   - Cancel and Back Buttons on Configuration Manager Pages
   - Navigational Aids for Tables
   - SnapShots Tab
   - Migration Tab
   - Transactions Tab
   - System Configuration Tab
   - Messages in the Configuration Manager

Logout Link

The Logout link appears in the upper-right corner of Configuration Manager pages. You select the Logout link to conclude your session.

Cancel and Back Buttons on Configuration Manager Pages

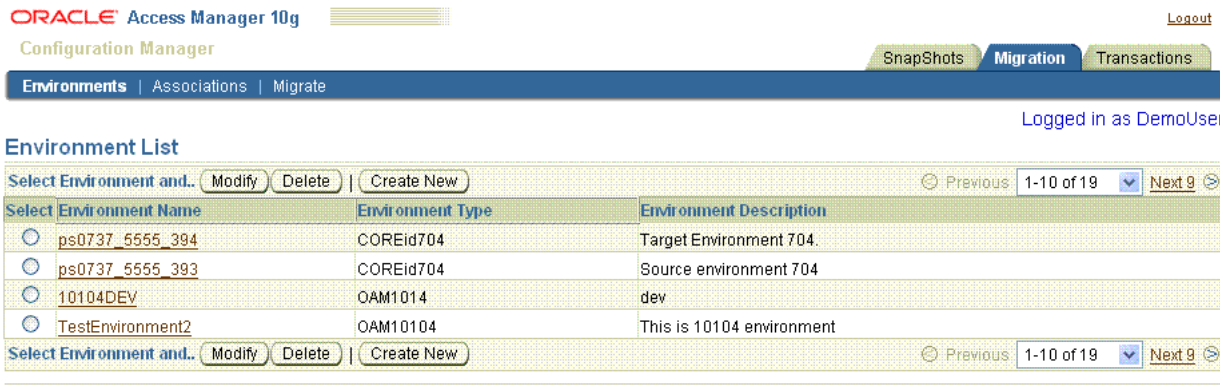
A Cancel button is provided on a number of Oracle Access Manager Configuration Manager pages. When you click Cancel, the current operation is terminated without completion and you are returned to the originating page for the function. For example if you cancel a migration operation, you are returned to the Select Logical Object Types to Compare page.

A Back button is included on some Oracle Access Manager Configuration Manager pages. When you click the Back button you are returned to the previous page. This is similar to using the Back button in the Web browser itself. For example if you click Back while viewing environment details, you are returned to the Environment List page.

Navigational Aids for Tables

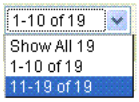
When you have more than one environment, association, snapshot, or transaction the corresponding list page itemizes information in a table. Figure 2–15 shows a typical list page and table details.

Figure 2–15 Navigational Aids for Tables



When a table contains less than 10 items, all are visible at one time. If a table contains more than 10 items, navigational aids are included. For example, the table in Figure 2–15 includes navigational aids at the top-right side of the table:

- **Previous**: Click Previous to return (go back) to the previous page.
- **Next:** Click Next to proceed (go forward) to the next page.
- **List**: Select a specific range of items from the list, or select Show All to display all the rows in the table.

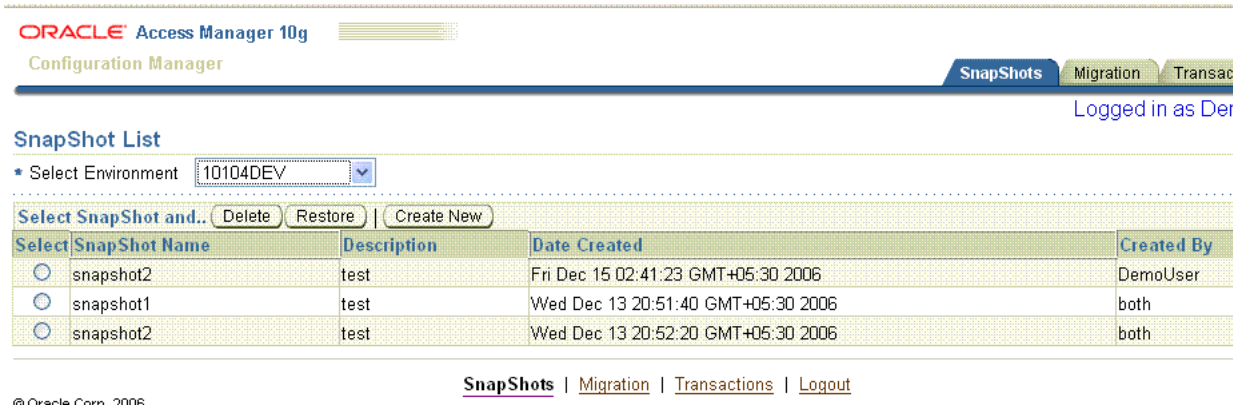


SnapShots Tab

The SnapShot function enables you to create a backup copy of the entire `oblix` tree in an LDAP directory of one of your environments. When you select the SnapShots tab, the SnapShot List page appears. From here, you can create a new snapshot or select a snapshot to restore or delete a snapshot.

Details for existing snapshots of the selected environment are organized in a table as shown in Figure 2–16. The table is empty until you select an environment from the Select Environment list.

Figure 2–16 Snapshot Tab

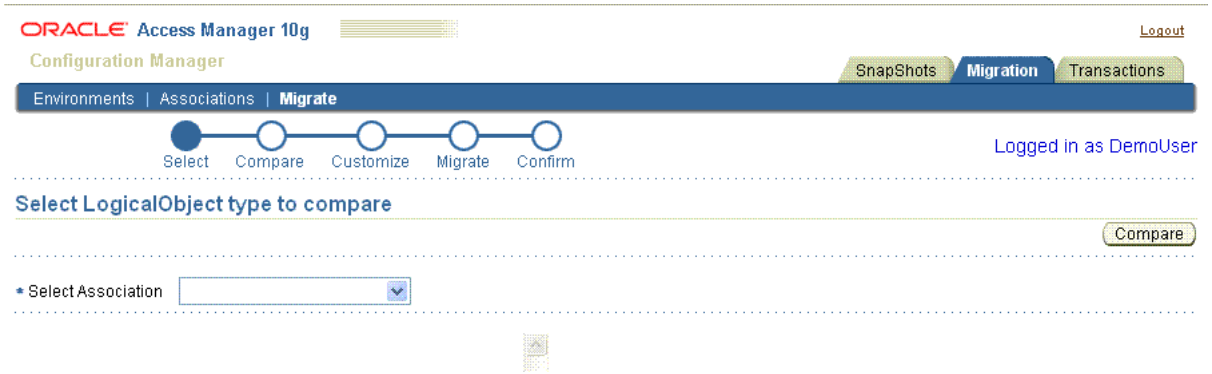


For more information, see "Making and Managing Snapshots" on page 3-38.

Migration Tab

Figure 2–17 shows the Migration tab. Related functions are available on secondary tabs: environments, Associations, Migrate. The Migrate secondary tab includes a progress indicator, as shown inFigure 2–17.

Figure 2–17 Migration Tab, Secondary Tabs, and Migrate Progress Indicator



You choose the corresponding secondary tab to perform tasks that involve:

- **Environments**: From this secondary tab you can create, view, modify, or delete details about existing environments. Before you can migrate data, you must add at least two environments to the Configuration Manager: one to use as the source and one to use as the target.

  For more information, see "Adding and Managing Environment Details in the Configuration Manager" on page 3-4.

- **Associations**: From this secondary tab you can create, view, modify, or delete details about directory associations. Before you can migrate data, you must create an association between two environments defined in the Configuration Manager: one to use as the source and one to use as the target.

  For more information, see "Creating and Managing Associations" on page 3-12.

- **Migrate**: After defining environments and forming an association, you can migrate configuration data using this secondary tab. You can migrate data directly using Oracle Access Manager Configuration Manager. Alternatively, you may choose to export data to an LDIF file and then use an external utility to import the data offline.

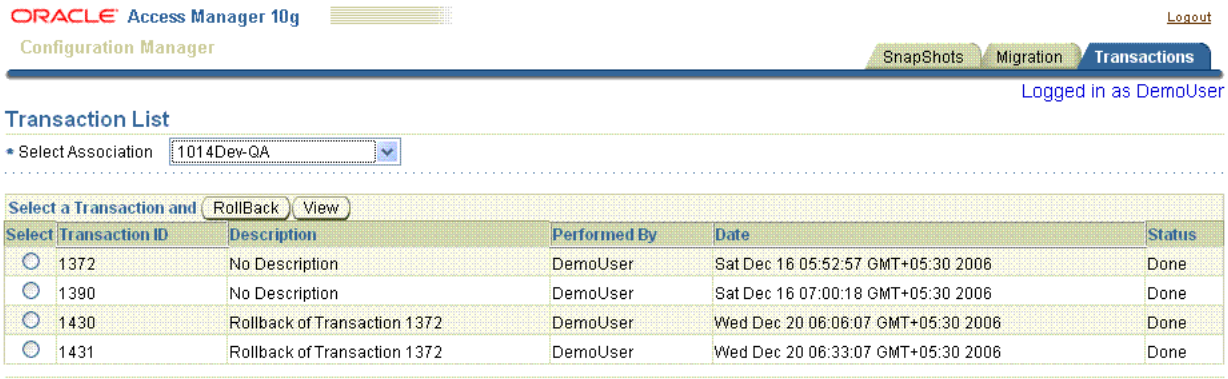
  For more information, see "Migrating Data from the Source to the Target" on page 3-43.

Transactions Tab

A transaction record is created automatically each time you migrate data using Oracle Access Manager Configuration Manager. A transaction ID is assigned automatically when the record is created. You can provide an optional transaction description.

When you select the Transactions tab, the Transactions List page appears. After selecting an association, all related transaction records are organized in a table as shown in Figure 2–18. The table is empty until you select an association.

Figure 2–18 Transactions Tab



You can view details for the record or view specific changes made during the transaction or roll back changes made during the transaction.

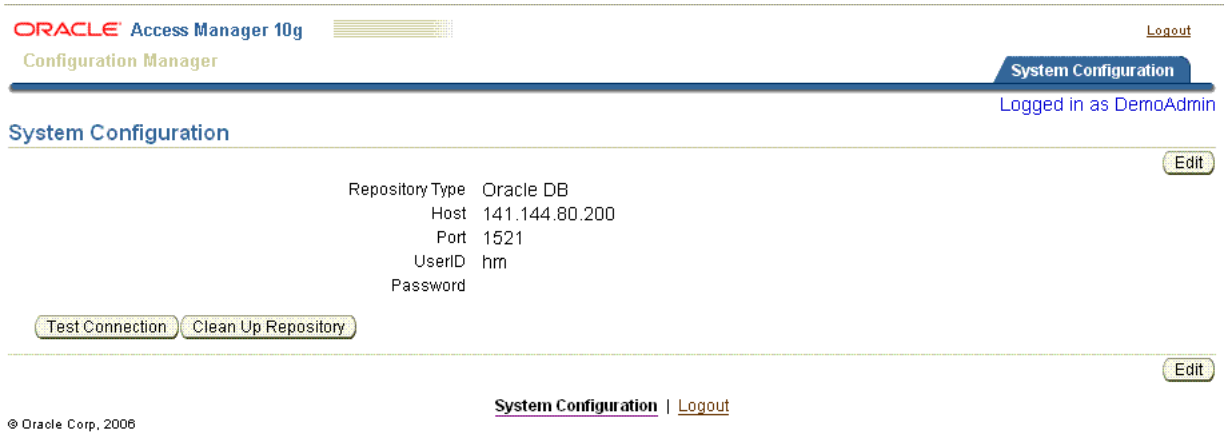
For more information about transactions and rolling back changes, see Chapter 5.

System Configuration Tab

A repository is required to contain details about directory environments and associations, snapshot content, audit details, migration transaction data, and any optional LDIF files you may choose to create using Configuration Manager.

Only when you log in as an individual with `HMAdmin` privileges, is the System Configuration tab available as shown in Figure 2–19. Until a repository is defined in the Configuration Manager, the form is empty.

Figure 2–19 System Configuration Tab



From the System Configuration tab, an individual with `HMAdmin` privileges can perform the following repository-related tasks in the Configuration Manager:

- **View**: Repository details are displayed automatically whenever the System Configuration tab is selected. The form is empty until a repository is defined in the Configuration Manager.
- **Edit**: Enables you to add or alter repository details. Repository details must be added before migration tasks can be performed.
- **Test Connection**: Ensures that the repository is accessible.
- **Cleanup Repository**: Clears the data in Oracle Access Manager Configuration Manager repository tables.
- **Upload Schema**: Appears only when there is no Oracle Access Manager Configuration Manager schema present in the Oracle Database repository.

  For a successful schema upload, the database user needs the following system privileges: Create Table, Create Sequence, Create Trigger, and Create Procedure.

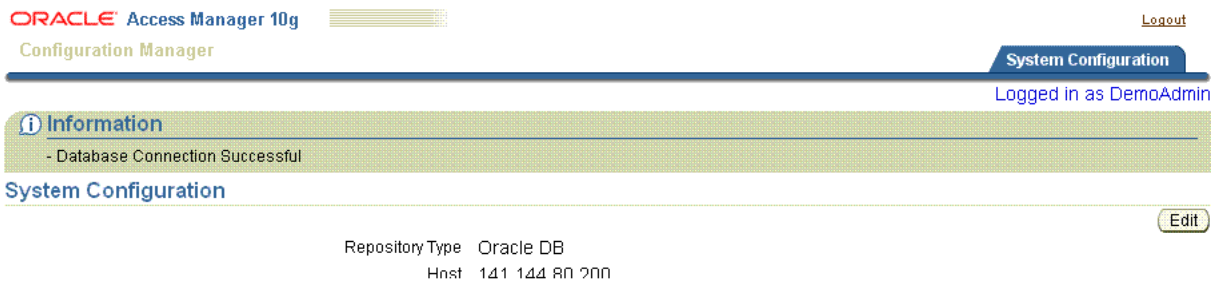
  For more information about System Configuration functions, see "Adding Repository Details in the Configuration Manager" on page 2-29.

Messages in the Configuration Manager

There are several types of messages that may appear when working with Oracle Access Manager Configuration Manager:

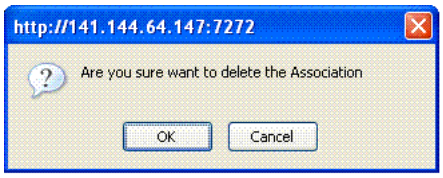
- **Informational or Confirmation Messages**: Confirm that an operation completed successfully. Informational messages appear near the top of the page as shown in Figure 2–20. In this example, the Test Connection operation was used for the repository. Upon completion, you are returned to the System Configuration page where a message confirms the success of the operation.

Figure 2–20 Informational Message



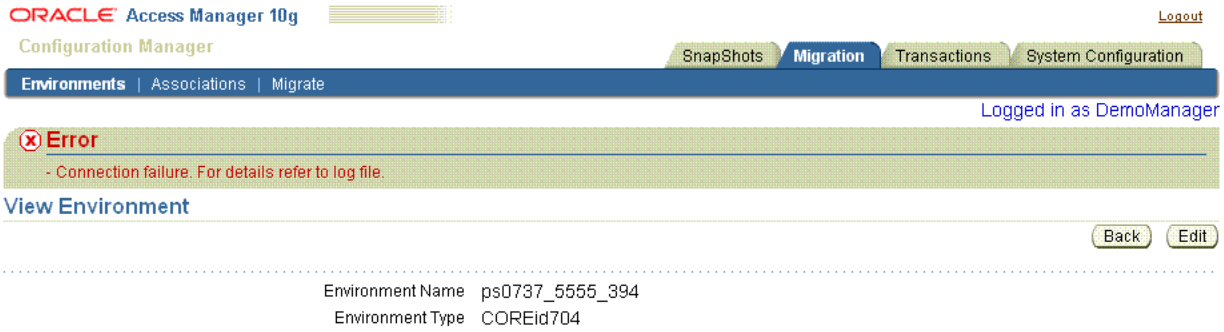
- **Request for Action or Verification**: Required before critical and irreversible operations are completed. For example, your verification is needed before deleting an environment or association or transformation rule. A window like the one in Figure 2–21 asks for your confirmation. You click OK to verify and complete the operation, or Cancel to terminate the operation without completing it.

Figure 2–21 Typical Request for Your Action



- **Error Messages**: Announce a problem when an operation cannot be completed successfully. Error messages take the form shown in Figure 2–22 and include information to help you assess the problem and recover.

Figure 2–22 Typical Error Message



Adding Repository Details in the Configuration Manager

A repository is required to contain details about directory environments and associations, snapshot content, audit details, migration transaction data, and any optional LDIF files you may create using Configuration Manager. This section describes how to ensure that the Configuration Manager can communicate with its repository.

Before starting activities in this section, confirm that the prerequisites described in Table 2–5 are completed.

Table 2–5 Repository Prerequisites

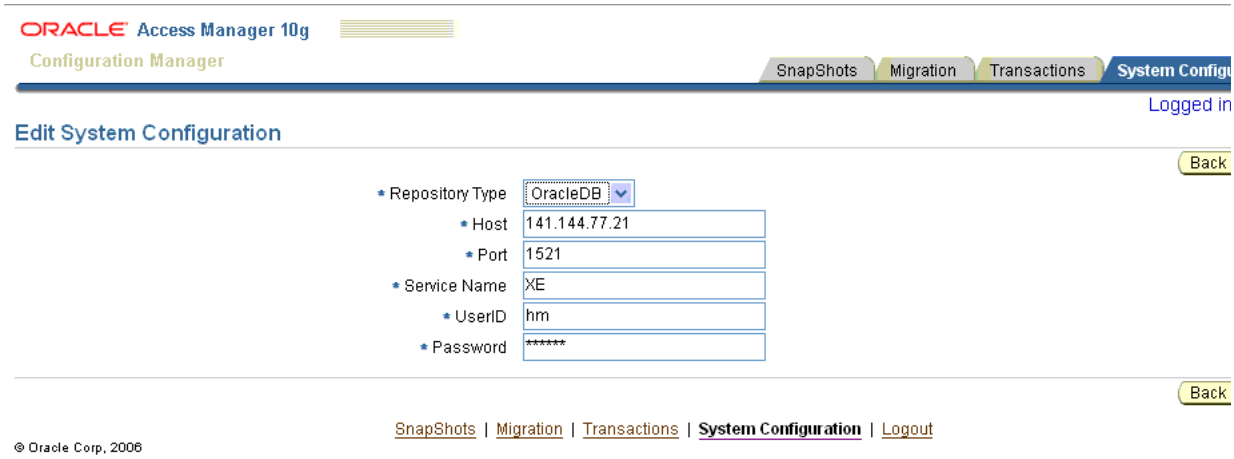
Confirm	Prerequisite Task	Look inLook in
	Assign Configuration Manager administrator role `HMAdmin` to individuals using OC4J	Assigning Configuration Manager Administrator and User Roles in OC4J on page 2-16

From the System Configuration page, you must click the Edit button and enter details for your repository. There is no Add button for the System Configuration tab. Sample details that you need to supply are shown in Figure 2–23. If you log in with *only* `HMUser` privileges, the System Configuration tab does *not* appear.

For a successful schema upload, the database user needs the following system privileges.

- Create Table
- Create Sequence
- Create Trigger
- Create Procedure

Figure 2–23 A Completed Edit System Configuration Page



To add repository details to Oracle Access Manager Configuration Manager

1. Enter Oracle Access Manager Configuration Manager, if you haven't already done so. For example:

   `https://hostname:port/ocm`

   In the sample URL, *hostname* refers to computer that hosts the Configuration Manager; *port* refers to the HTTP port number on which the Configuration Manager host listens; and /ocm refers to Web Module Context Root specified on the Application Attributes page while deploying the Oracle Access Manager Configuration Manager application.

   The Welcome page appears.

2. Log in as an individual with `HMAdmin` privileges, as defined in OC4J in the previous procedure.

HMAdmin_Name
Passwword

3. Click the System Configuration tab on the right side of the page.

> **Note:** Only users with `HMAdmin` privileges defined in OC4J for this application will see the System Configuration tab.

4. On the System Configuration page, click the Edit button.

   Edit

5. On the Edit System Configuration page, enter appropriate information to identify details for your Configuration Manager repository. For example:

   - **Repository Type**: You would ordinarily select your repository type from the list. However, only Oracle Database is listed because this is the only supported repository type.
   - **Host**: Your Oracle Database Host Name expressed as either the full DNS hostname or an IP address.
   - **Port**: Port number on which the Oracle Database host communicates.
   - **Service Name**: The Oracle Database service name as defined in the db.properties file. For more information, see "Defining the Oracle Database Service Name" on page 2-22.
   - **UserID**: The Oracle Database Administrator userID.
   - **Password**: The password for the Oracle Database Administrator userID. There are no password restrictions.
   - Click Save to retain this information (otherwise, click the Back button).

     The System Configuration page returns and includes a Test Connection button that you can use to ensure that the repository is accessible from the Configuration Manager.

6. Click the Test Connection button to ensure that this repository is accessible to the Configuration Manager. For example:

   Test Connection

   An informational message that appears before the repository details confirms that the database connection was successful.

7. Proceed as follows:

   - **Connection Successful**: An informational message appears declaring the operation was a success. You are ready to upload the schema as described in step 8.

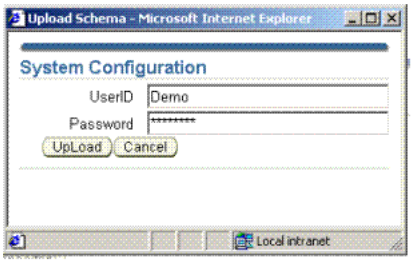
     For a successful schema upload, the database user needs the following system privileges: Create Table, Create Sequence, Create Trigger, and Create Procedure.
   - **Connection Not Successful**: An error message appears. In this case, confirm that all repository details are accurately entered (edit them if needed); confirm that the Oracle Database instance is running; test the connection again, then proceed with the next step to upload the schema.

8. **Upload Schema**: When you add repository details you need to upload the Configuration Manager schema as follows:

   a. Click the Upload Schema button. For example:

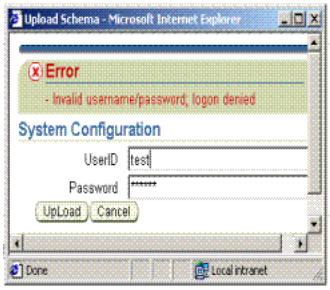
      Upload Schema

   b. In the Upload Schema window, enter the directory administrator's UserID and password, then click Upload to complete the operation (or Cancel to terminate the operation without completion).



9. Proceed as follows:

   - **Schema Upload Successful**: A message informs you that the database is configured successfully and you are ready to prepare for and perform migration tasks as described in Chapter 3.
   - **Schema Upload Not Successful**: In this case, a message like the one here appears. Confirm that you have the appropriate system privileges to create a table, create a sequence, create a trigger, and create a procedure; retry the upload, then proceed to Chapter 3.



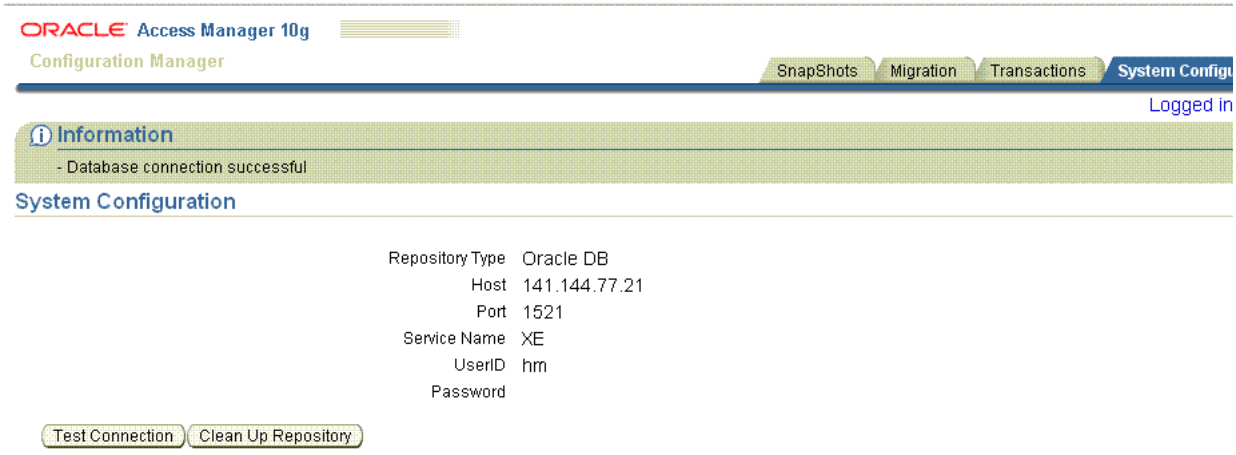
After adding repository details to Oracle Access Manager Configuration Manager and uploading the schema, the Configuration Manager is ready to use. For more information about adding environment details, forming associations, creating snapshots, and migrating data, see Chapter 3.

Ensuring the Repository is Available to the Configuration Manager

Data can be written to the repository only when it is live and accessible. Any individual with `HMAdmin` privileges can use the Test Connection procedure to ensure that the repository is available to the Configuration Manager.

After the operation completes successfully, an informational message confirms the status as shown in Figure 2–24.

Figure 2–24 Informational Message on the System Configuration Page



Note: Only users with `HMAdmin` privileges defined in OC4J have access to the System Configuration tab. If you log in as a user with only `HMUser` privileges, the System Configuration tab does *not* appear.

To confirm that the Configuration Manager repository is available

1. From the Oracle Access Manager Configuration Manager home page, log in as a user with `HMAdmin` privileges, then click the System Configuration tab on the right side of the page:

   `HMAdmin_Name`
   `Passwword`

   System Configuration

2. On the System Configuration page, click the Test Connection button then review the informational message to confirm that this repository is accessible.

   Test Connection

3. Proceed as follows:

   - **Connection Successful**: An informational message appears and you are ready to continue with activities in this chapter.
   - **Connection Not Successful**: An error message appears. In this case, take the following actions:
     - Confirm that the database service name is properly specified for this repository, as described in "Defining the Oracle Database Service Name" on page 2-22.
     - Contact the Oracle Database administrator to confirm that the Oracle Database instance is running, test the connection again

Configuring Logging for Oracle Access Manager Configuration Manager

You perform the following activities to configure logging for Oracle Access Manager Configuration Manager.

Oracle Access Manager Configuration Manager uses Oracle Diagnostic Logging for Java (ODL) to produce log files. The ODL library is incorporated into the Configuration Manager in ojdl.jar file, which is part of the Oracle Access Manager Configuration Manager deployment.

Log File Naming: The current ODL log file naming standard is followe, which means that each new log file that is generated is named log.xml. The generated log file is stored as:

$*OC4J_Home*/j2ee/home/log/OAMCMLogs/log.xml

Log File Rotation: Log rotation is automatic and based on file size. This means that log files rotate automatically when the current log reaches a certain size. The maximum limit for log file size is 100 MB. When the current file reaches the size limit, a new file is created as log.xml and the content in the earlier version is archived with a different name. Archived log files are named as log*index*.xml, where *index* is a number. Older archived files have a lower index number: log1.xml is the oldest, log2.xml is the next oldest, and so on.

To configure logging for Oracle Access Manager Configuration Manager, you must add specific logger and log handler details based on (ODL specifications) to the following file (as indicated in the following procedure):

OC4J_Home/j2ee/home/config/j2ee-logging.xml

The following (**bold**) HMLogger entries must be included for Configuration Manager log file rotation (the value of the `maxFileSize` is in bytes):

```
<property name='maxFileSize' value='10485760'/>
<property name='maxLogSize' value='104857600'/>
```

For more information about log files, see "Accessing and Using the Log File" on page B-1.

To configure logging for Oracle Access Manager Configuration Manager

1. Locate the following file and open it for edit:

   OC4J_Home/j2ee/home/config/j2ee-logging.xml

2. Change the encoding to UTF-8, as follows:

   ```
   <?xml version="1.0" encoding="UTF-8"?>
   ```

3. Add the following log handler details (in **bold**) immediately before the <loggers> section and Default Logger information:

   ```
     <!-HM Application specific log Handler -->
   <log_handlername="HMLog-Handler"
     class="oracle.core.ojdl.logging.ODLHandlerFactory">
       <property name="path" value="../log/OAMCMLogs"/>
       <property name="maxFileSize" value="10485760"/>
       <property name="maxLogSize" value="104857600"/>
       <property name="encoding" value="UTF-8"/>
   </log_handler>
  </log_handlers>
   ```

4. Add the following logger details (in **bold**) immediately after </logger> in the Default Logger section:

   ```
     <!-- HM Application logger -->
   <logger name="com.oracle.hm.log.HMLogger" level="ALL"
     useParentHandlers="false">
   ```

```
    <handler name="HMLog-Handler"/>
  </logger>
 </loggers>
</logging_configuration>
```

5. Save the file; the details that you have added will be used when generating log files for Oracle Access Manager Configuration Manager.

3

Migrating Configuration Data Changes

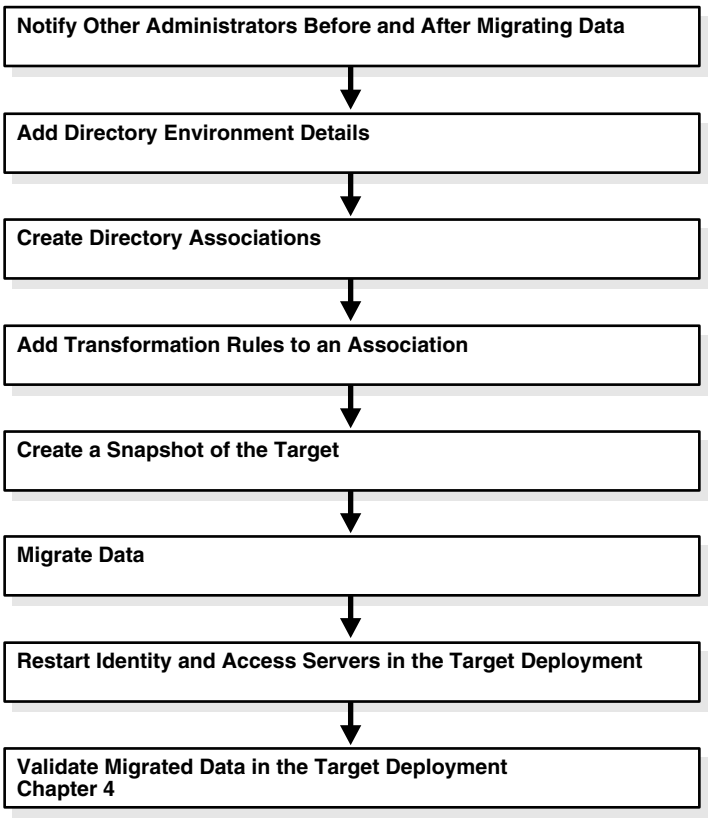
This chapter provides the information that you need as you prepare to migrate configuration data from a source LDAP directory (environment) to a target. Topics in this chapter include:

About Migrating Data

After activities in Chapter 2 have been performed, Oracle Access Manager Configuration Manager is ready to use for migration activities.

Figure 3–1 provides an overview of the procedures involved in preparing for and migrating data using Oracle Access Manager Configuration Manager. Additional information follows the figure.

Figure 3–1 Preparing for and Migrating Data Using Configuration Manager



Task overview: Migrating data includes

1. **Notifying Other Administrators**: Recommended both before and after any data migration.
2. **Adding Environment Details to the Configuration Manager**: Required before you can form an association.
3. **Creating a Directory Association**: Required before migration.
4. **Adding and Managing Optional Transformation Rules**: Optional and applied automatically during migration.
5. **Creating a Snapshot**: Recommended before any data migration.
6. **Migrating Data from the Source to the Target**.
7. **Restarting Servers After Migration**: Required after data migration.
8. **Validating Migration Success**: Recommended to ensure that everything in the target deployment works as expected, and described in Chapter 4.

You *cannot* use Oracle Access Manager Configuration Manager to migrate data from a release 7.0.4 deployment to a release 10*g* (10.1.4.0.1) deployment *nor* vice versa. Oracle Access Manager Configuration Manager performs automatic checks at strategic points to prohibit you from making a mistake. For more information, see "Deployment Support and Interoperability" on page 1-16.

Accessing the Configuration Manager

The procedure in this section explains how to access Oracle Access Manager Configuration Manager.

You must log in with appropriate rights for the tasks that you want to perform using the Configuration Manager. There are two types of OC4J roles for the Configuration Manager, which must be defined by the OC4J administrator:

- `HMAdmin` role is required to perform system configuration activities, including testing the connection with the repository.
- `HMUser` role enables you to perform all activities *except* system configuration.

Before you start this procedure, confirm that all prerequisites described in Table 3–1 have been performed.

Table 3–1 Oracle Access Manager Configuration Manager Access Prerequisites

Confirm	Prerequisite Tasks	Look in
	Set up a repository for Oracle Access Manager Configuration Manager and install OC4J.	Setting Up a Repository and Installing OC4J on page 2-5
	Deploy Oracle Access Manager Configuration Manager as an OC4J application.	Deploying the Configuration Manager on page 2-12
	Assign OC4J roles to individuals to provide access privileges to the Configuration Manager. Check with your OC4J administrator to learn your login ID and password for the Configuration Manager.	Assigning Configuration Manager Administrator and User Roles in OC4J on page 2-16
	Add repository details to the Configuration Manager.	Adding Repository Details in the Configuration Manager on page 2-29

To access the Configuration Manager

1. Access your Configuration Manager home page URL as usual:

   ```
   https://hostname:port/ocm/faces/index.jsp
   ```

   In this URL example, *hostname* refers to the computer that hosts the Configuration Manager; *port* refers to the HTTP port number on which the Configuration Manager host listens; /ocm refers to the Web Module Context Root specified on the Application Attributes page while deploying Oracle Access Manager Configuration Manager; and faces/index.jsp connects to the Configuration Manager application's Login page.

   The Login page appears.

2. Log in as an individual with `HMUser` privileges (defined in OC4J) for the activities that you intend to perform. For example:

   ```
   HMUser_Name
   Password
   ```

3. Proceed with the activities in this chapter.

Notifying Other Administrators

Oracle recommends that you schedule specific migration windows for promoting changes and restarting servers. Further, Oracle recommends that you notify other administrators both before and after migrating data in a deployment for which they have responsibility.

> **Note:** Notifying other administrators is a manual task that must be performed without the aid of the Configuration Manager.

Your migration team can collect and confirm details regarding the logical object types (or logical objects) that will be migrated, the source and target directories, when backups (snapshots) will be made. The migration team can send this information to others to ensure dedicated coordination. When the migration is complete, you can notify the same administrators so they can assist in restarting servers and validation procedures.

To notify other administrators

1. Create a list of all administrators in any deployment that will be affected by the change.
2. Create an e-mail that includes all relevant details for the administrator, deployment, and situation. For example:

```
ANNOUNCING DATA MIGRATION THAT MIGHT AFFECT YOUR DEPLOYMENT:

CONFIGURATION DATA WILL BE MIGRATED FOR:
Oracle Access Manager 10g (10.1.4.0.1)
(OR Oracle COREid Release 7.0.4, if this is your deployment)

WHEN:  Date and time

SOURCE DIRECTORY: DNS hostname
TARGET DIRECTORY:  DNS hostname

A SNAPSHOT OF THE TARGET DIRECTORY WILL BE MADE: Date and time

MIGRATED CHANGES MUST BE PROPAGATED TO ANY REPLICAS.

IDENTITY AND ACCESS SERVERS MUST BE RESTARTED AFTER DATA MIGRATION TO
ENSURE DATA SYNCHRONIZATION.
```

3. Before data migration, send the e-mail to all administrators who might be affected.
4. Send a follow-up e-mail to all administrators after the migration to announce what was done.

Adding and Managing Environment Details in the Configuration Manager

This section provides step-by-step procedures to add and manage environment details in the Configuration Manager. The Configuration Manager repository must be online for these activities. Oracle recommends that the source and target environments are also online.

> **Note:** Any environment that is involved when making a directory snapshot, migrating data, or rolling back a transaction *must* be live and online. To ensure that an environment is available to the Configuration Manager, see "Testing the Environment Connection" on page 3-12.

Table 3–2 shows the tasks that must be completed before you can perform activities to add and manage directory environment details in the Configuration Manager. The

task overview that follows outlines details about managing environments using the Configuration Manager.

Table 3–2 Environment Prerequisites

Confirm	Prerequisite Tasks	Look in
	Setting Up a Repository and Installing OC4J	Chapter 2 on page 2-5
	Deploying the Configuration Manager	Chapter 2 on page 2-12
	Assigning Configuration Manager Administrator and User Roles in OC4J	Chapter 2 on page 2-16
	Defining the Oracle Database Service Name	Chapter 2 on page 2-22
	Adding Repository Details in the Configuration Manager	Chapter 2 on page 2-29
	Ensuring the Repository is Available to the Configuration Manager	Chapter 2 on page 2-32
	Configuring Logging for Oracle Access Manager Configuration Manager	Chapter 2 on page 2-33

Task overview: Managing environment details for existing deployments includes

1. Adding Environment Details to the Configuration Manager: Required before you can form an association and migrate data
2. Viewing Environment Details in the Configuration Manager
3. Modifying Environment Details in the Configuration Manager
4. Deleting Environment Details in the Configuration Manager
5. Testing the Environment Connection

Adding Environment Details to the Configuration Manager

The procedure in this topic explains how to add environment details to the Configuration Manager. Any individual with `HMUser` privileges can add environment details. The repository for Oracle Access Manager Configuration Manager must be online. Oracle recommends that the environment (LDAP directory) also be online.

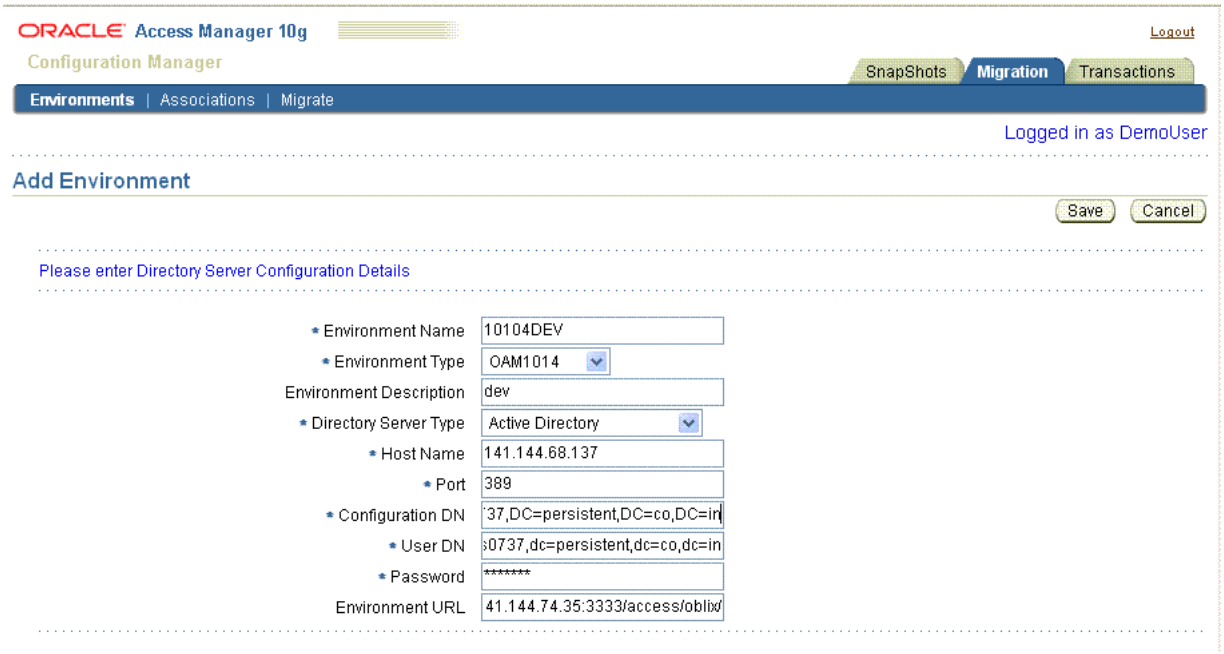
Note: After adding details for at least two LDAP directory environments, you can form an association that specifies a source and target for data migration.

Failover and Load Balancing: Oracle Access Manager Configuration Manager does *not* support directory failover or load balancing. For each existing deployment, the Configuration Manager writes to *only* a single master LDAP directory and reads from *only* a single master or replica server.

Replicated Environments: In a replicated directory environment, you must add details for *only* the master directory (the one on which write operations take place) as the target environment. Otherwise the objects that you select for migration cannot be written into the target and migration will fail. After migrating configuration data to the master LDAP directory you must ensure that the changes have fully propagated to the replicas before restarting Identity Servers and Access Servers.

When you click the Create New button from the Environment List page, the Add Environment page appears. A filled in sample is shown in Figure 3–2. Your environment will differ.

Figure 3–2 Add Environment Page



Lists are provided from which you can select the environment type (OAM 1014 or COREid704) and directory type. In this example, the environment type is OAM1014.

The Add Environment page provides fields where you can enter other information, including Environment Name, optional Description, Host Name and Port, Configuration DN, User DN, Password, and the URL for the LDAP Directory environment. When defining an environment name and description, you can use any combination of uppercase and lowercase alphanumeric characters, as well as spaces and punctuation.

If the environment is SSL-enabled, be sure to specify that on the Add environment page. For more information, see the following procedure.

To add details about an existing environment

1. From Oracle Access Manager Configuration Manager, click the Migration tab, then click Environments.

   Migration, Environments

2. On the Environment List page, click the Create New button.

   Create New

3. On the Add Environment page, provide the information for this specific directory server using the guidelines in this procedure overview. For example:

   - **Environment Name**: Enter a unique and descriptive name for this directory server. You might want to include details about the environment, hostname, port, or other identifying characteristics. For example:

     10104DEV

   - **Environment Type**: Select the type of environment for which this directory server is installed (either release (10*g* (10.1.4.0.1) or release 7.0.4).

     OAM1014

- **Environment Description**: Enter a brief optional statement that further identifies this directory and its environment. For example:

  dev

- **Directory Type**: Select the type of directory server from those listed. For example:

  Active Directory

- **Host Name**: Enter the complete DNS hostname (DNS_hostname.domain.com) or IP Address of the computer where this directory is installed. For example:

  141.144.68.137

- Port: Enter the port number on which this directory server communicates.

  389

- **Configuration DN**: Enter the configuration DN for Oracle Access Manager 10*g* (10.1.4.0.1), or Oracle COREid Release 7.0.4, data. For example:

  OU=oblix,OU=company1,DC=obps0737,DC=persistent,DC=co,DC=in

  Note: The configuration DN must start from the `oblix` node.

- **User DN**: Enter the directory administrator ID for this environment (LDAP directory). For example:

  cn=administrator,cn=users,dc=obps0737,dc=persistent,dc=co,dc=in

- **Password**: Enter the directory administrator password: For example:

  Your_password

- **Environment URL**: The URL to the LDAP directory. For example:

  http://141.144.74.35:3333/access/oblix/

  For more information, see "Viewing Environment Details in the Configuration Manager" on page 3-8.

4. **Enable SSL**: If Secure Sockets layer (SSL) is enabled for this directory, click Enable SSL at the bottom of the page, then load a certificate for this directory using the following steps. For example:

   a. Check the box beside Enable SSL.

   b. Click the add Certificate link (beside the Enable SSL check box) to display the Upload Certificate dialog box then fill in requested details. For example:

   – **CA Certificate File**: Enter (or browse and select) the absolute path to the CA Certificate file for this directory.

   – **Keystore Password**: Enter the password for the keystore file.

   – Click the Upload button to obtain the certificate (or Cancel to dismiss the dialog box without uploading the certificate).

   c. Take one of the following actions:

   – **Certificate Upload Successful**: You are returned to the page where you started. In this case, proceed to Step 5.

- **Certificate Upload Not Successful**: An error message appears to help you solve the problem. In this case, click the Cancel button on the error window, verify the location of the files and password, and complete the certificate steps again.

5. Click Save when you have finished filling in the details for this directory server.

   Save

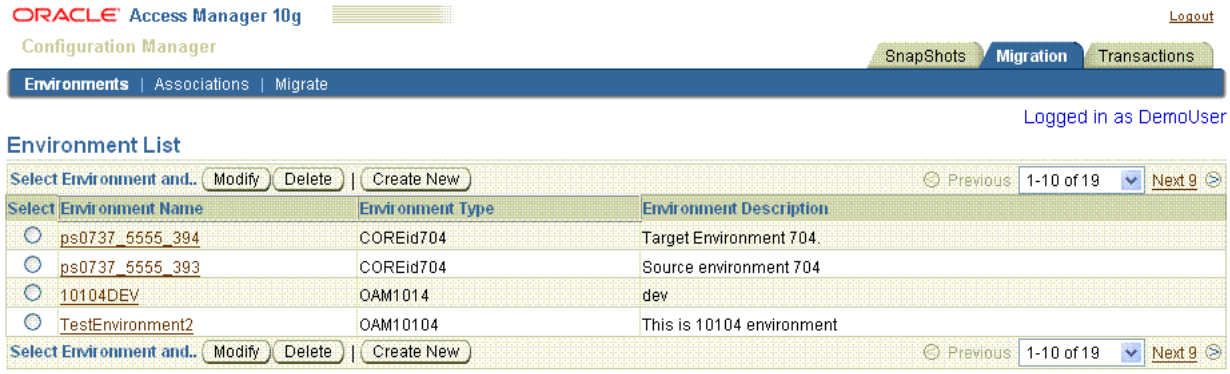
6. Repeat the steps in this procedure to add environment details for at least one other LDAP directory in another deployment of the same release.

Viewing Environment Details in the Configuration Manager

The procedure in this topic explains how you view environment details that were added to the Configuration Manager. This activity can be performed by any individual with `HMUser` privileges.

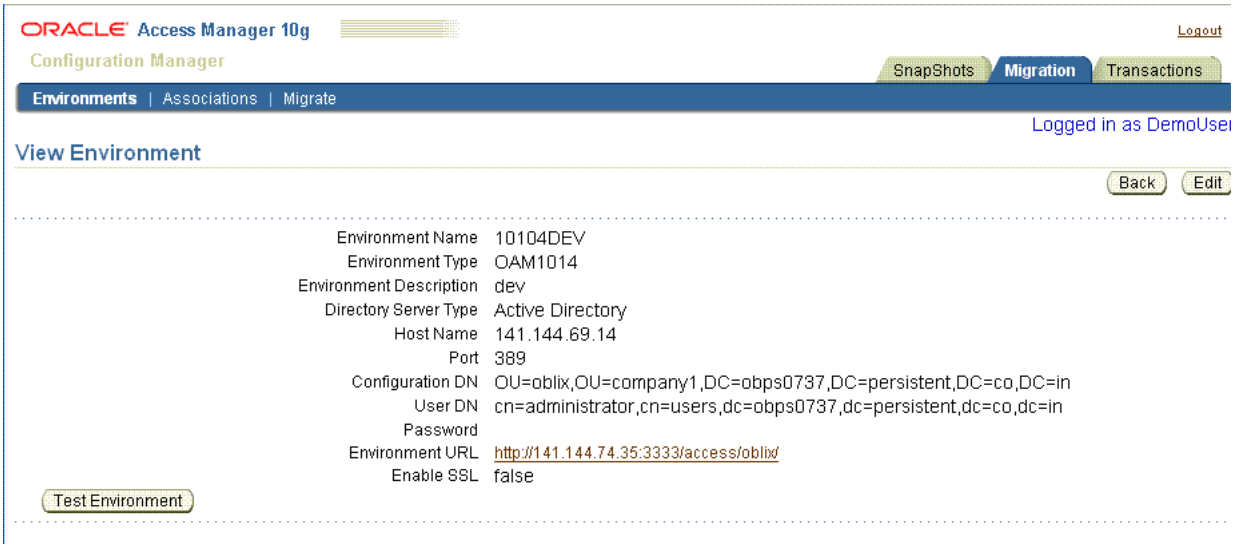
The Environments List page appears as shown in Figure 3–3 when you click the Migrate tab, then click the Environments secondary tab. If there are no go to "Adding Environment Details to the Configuration Manager" on page 3-5.

Figure 3–3 Environments List Page



When you click a name in the Environment Name column, the View Environment page appears as shown in Figure 3–4. Details about this page follow the figure.

Figure 3–4 View Environment Page



The View Environment page includes the following types of information:

- **Environment Name**: The unique name that was entered when details about this directory server were added to the Configuration Manager (10104DEV, for example).
- **Environment Type**: The release for which this directory server is installed (OAM1014, for example).
- **Environment Description**: An optional statement that further identifies this directory and its deployment (dev, for example).
- **Directory Type**: The supported directory server type (Active Directory in this example).
- **Host Name**: The DNS hostname of the computer where this directory is installed (the full IP address, in this example).
- **Port**: The port number on which this directory server communicates (389 in this example).
- **Configuration DN**: The bind DN for configuration data for the specified environment (in this example, it is `OU=oblix,OU=company1,DC=obps0737,DC=persistent,DC=co,DC=in`).

  The configuration DN is similar to the searchbase for user data. The configuration DN must be specified to identify the node in the DIT under which the Oracle Access Manager schema and configuration data are stored. For more information about its use and location within Oracle Access Manager 10*g* (10.1.4.0.1), or Oracle COREid Release 7.0.4, deployments, see the corresponding *Installation Guide* as described in "Related Documents" on page x.
- **User DN**: The administrator ID, also known as a bind DN or root DN, for the for the specified environment (in this example it is `cn=administrator,cn=users,dc=obps0737,dc=persistent,dc=co,dc=in`)

  This directory account should have Read, Write, Add, Delete, Search, Compare, and Self-write permissions. The method to create a user with these privileges varies among directory vendors. See your directory documentation for details. For

more information about its use and location within Oracle Access Manager 10*g* (10.1.4.0.1), or Oracle COREid Release 7.0.4, deployments see the corresponding *Installation Guide* as described in "Related Documents" on page x.

- **Password**: The User DN directory administrator password.
- **Environment URL**: The URL to the LDAP directory.
- **Enable SSL**: True if enabled; False if not enabled.

To view environment details that were added to the Configuration Manager

1. From Oracle Access Manager Configuration Manager, click the Migration tab, then click Environments to display the Manage Environment page. For example:

   Migration, Environments

2. In the Environment Name column, click the desired environment name to view details about the selected directory. For example:

3. From the View Environment page you can perform any of the following activities:
   - Click the Test Environment button to ensure that this directory is live and online.
   - Click the Back button to return to the Manage Environment page.
   - Click the Edit button to modify details for the selected directory. In this case, proceed to "Modifying Environment Details in the Configuration Manager" on page 3-10.

Modifying Environment Details in the Configuration Manager

Modifying environment details can be performed by any individual with `HMUser` privileges. The repository for Oracle Access Manager Configuration Manager must be online. Oracle recommends that the environment (LDAP directory) also be online.

You use the following procedure to modify existing environment details.For example, you might want to re-enter something that was stated incorrectly. In the Configuration Manager, you can alter all details except Environment Name and Environment Type.

For this operation you use the option in the Select column to choose the desired name; do not click the name itself. For information and guidelines about each entry, see "Adding Environment Details to the Configuration Manager" on page 3-5.

> **Note:** You cannot modify the environment name and environment type.

To modify details about a directory environment

1. From Oracle Access Manager Configuration Manager, click the Migration tab, then click Environments. For example:

   Migration, Environments

2. In the Select column, click the option beside the desired environment name, then click the Modify button. For example:

Modify

3. On the Modify Environment page, edit any details about this directory that you want to change.
4. Click Save when you have finished editing the details (or Cancel to terminate the operation before completion).

Save

Deleting Environment Details in the Configuration Manager

You can delete environment details in the Configuration Manager as described in the following procedure. However, you cannot delete an environment that is defined as part of an association.

Any individual with `HMUser` privileges can delete environment details. The repository for Oracle Access Manager Configuration Manager must be online. Oracle recommends that the environment (LDAP directory) also be online.

After deleting environment details in the Configuration Manager, the environment is no longer available for forming associations or migrating data.

For this operation you use the option in the Select column to choose the desired name; do *not* click the name itself. During this operation, you are asked to verify that this is what you want to do. When the operation is completed, you are returned to the Manage Environments page where an informational message notifies you that the selected items were deleted.

Note: If an environment is a part of an association, you must first delete the association and then delete the environment.

To delete environment details from the Configuration Manager

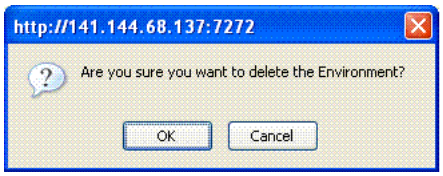
1. From Oracle Access Manager Configuration Manager, click the Migration tab, then click Manage Environments. For example:

Migration, Environments

2. Click the option beside the desired Environment Name, then click the Delete button. For example:

Delete

A message asks you to verify this is what you want to do before the operation is performed, as shown here.



3. Verify the removal by clicking OK in the message window (or Cancel to terminate the operation without completing it).

   OK

4. On the Manage Environments page, review the informational message to validate that the operation was successful and confirm that the environment details are no longer listed.

Testing the Environment Connection

The environment must be live and online during snapshot, migration, and transaction operations. Any individual with `HMUser` privileges can test an environment connection.

If there is any problem with the connection, notify the directory administrator.

To ensure the environment is live and online

1. From Oracle Access Manager Configuration Manager click the Migration tab, then click Environments:

   Migration, Environments

2. Click the desired name in the Environment Name column to view details. For example:

3. On the View Environment page, click the Test Environment button.

   Test Environment

4. Read the informational message to ensure that the environment connection is successful.

   - **Connection Successful**: Continue with activities that involve this directory.
   - **Connection Not Successful**: Notify the directory administrator. The directory must be live and online during snapshot, migration, and transaction operations.

Creating and Managing Associations

This section explains how to view, create, enable, disable, and delete a directory association using Oracle Access Manager Configuration Manager. Before proceeding, confirm that prerequisite activities outlined inTable 3–3 are completed.

Table 3–3 Association Prerequisites

Confirm	Prerequisite Task	Look in
	Add details for at least two environments (LDAP directories) to be used during data migration.	Adding Environment Details to the Configuration Manager on page 3-5

Any individual with `HMUser` privileges can perform activities in the following task overview. The repository for Oracle Access Manager Configuration Manager must be online. Oracle recommends that the environment (LDAP directory) also be online.

Task overview: Creating and managing directory associations includes

1. Viewing Settings for a Directory Association
2. Creating a Directory Association(required before you can migrate data)
3. Enabling or Disabling a Directory Association
4. Deleting a Directory Association

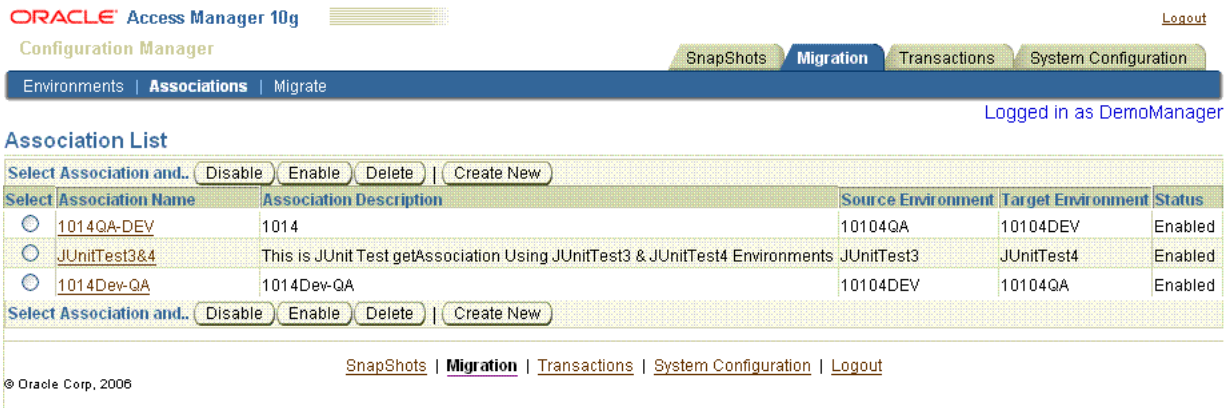
Viewing Settings for a Directory Association

You can view association settings as described in the following procedure. If you have not yet created an association, see "Creating a Directory Association" on page 3-15.

Any individual with `HMUser` privileges can view association settings. The repository for Oracle Access Manager Configuration Manager must be online. Oracle recommends that the environment (LDAP directory) also be online.

When you click the Associations secondary tab under the Migrate tab, the Association List page appears. A sample is shown in Figure 3–5. The table is empty when no associations exist in the Configuration Manager.

Figure 3–5 Association List Page



The Association List page provides several function buttons: Disable, Enable, Delete, Create New. Starting with the left-most column in the table, the Select column provides an option beside each name in the Association Name column. You click the option in the Select column that corresponds to the name of the association that you want to enable, disable, or delete.

The Association Name column provides a link that you can click to view details of that association. The Association Description column provides an optional description that was entered when this association was added. The Source Environment column and

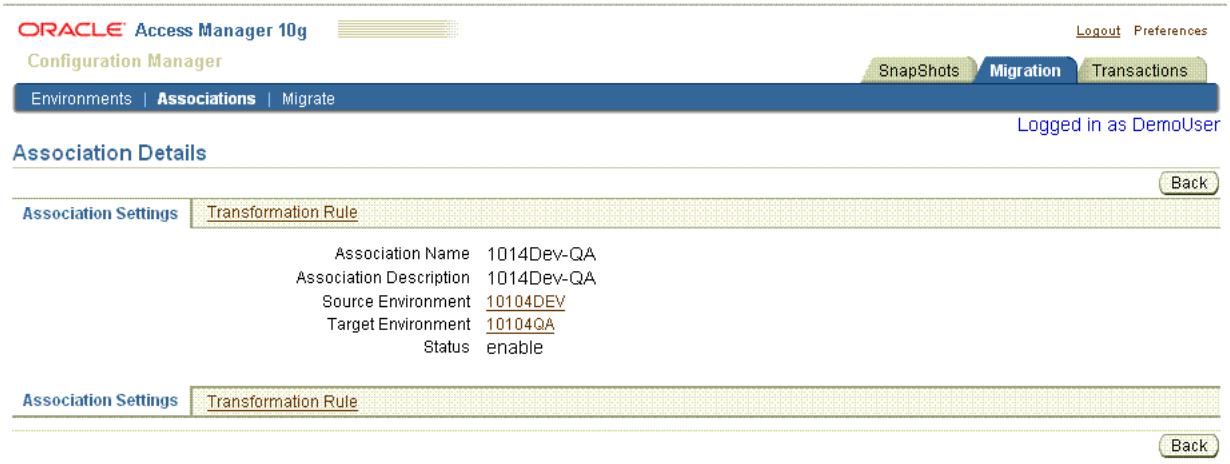
Target Environment column provide the names of the source and target LDAP directories that comprise the named association. The Status column identifies whether the association is enabled or disabled.

The following list provides more information about the information within each column:

- **Association Name**: The unique name entered to identify this associated directory pair.
- **Association Description**: A brief optional statement entered for this association.
- **Source Environment**: The name of the source environment (the LDAP directory that contains the data that you will migrate).
- **Target Environment**: The name of the target environment (the LDAP directory to which data will be migrated).
- **Status**: Enabled or Disabled. Each association is enabled automatically when created.

When you click an asociation name in the table, the Association Details page appears as shown in Figure 3–6. You find the same information for a single association on both the Association Details page and in the table on the Association List page. The Association Details page includes a sub tab that you can use to add a transformation rule as described in "Adding and Managing Optional Transformation Rules" on page 3-31.

Figure 3–6 Association Details Page



To view association settings

1. From Oracle Access Manager Configuration Manager, click the Migration tab, then click Association:

   Migration, Associations

2. On the Association List page, click a name in the Association Name column. For example:

3. On the Association Details page, view the settings for this directory pair.

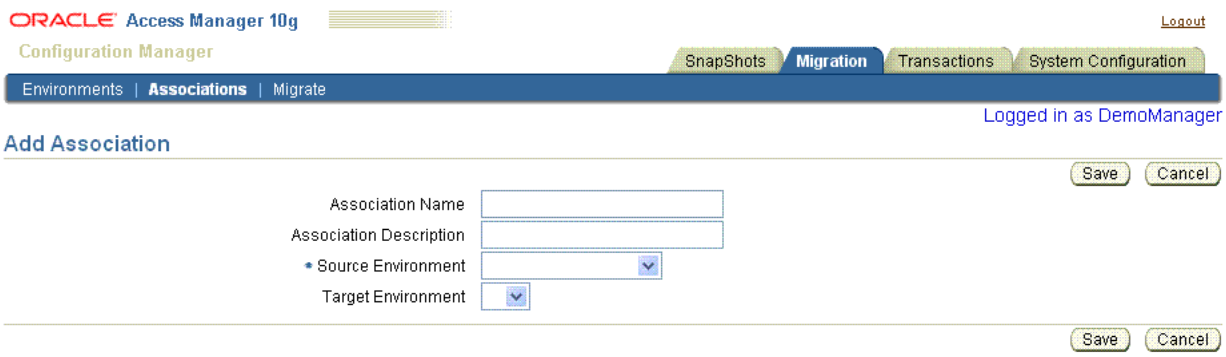
4. Click the Back button to return to the Association List page.
5. Proceed to the following topics, if desired:
   - Creating a Directory Association
   - Enabling or Disabling a Directory Association
   - Deleting a Directory Association
   - Adding and Managing Optional Transformation Rules

Creating a Directory Association

Data migration requires a directory association that specifies the migration path between a source and target environment. Any individual with `HMUser` privileges can create an association. The repository for Oracle Access Manager Configuration Manager must be online. Oracle recommends that the environment (LDAP directory) also be online.

When you click the Associations secondary tab under the Migration tab, the Association List page appears. You click the Create New button to display the Add Association page, which is shown in Figure 3–7.

Figure 3–7 Add Association Page



When you enter an association name and optional description, you can use any combination of upper and lower case alpha/numeric characters, as well as spaces and punctuation. Lists are provided from which you can select the source and target environments from those that have been defined in the Configuration Manager.

After you select a source environment, a list of possible target environments is established based on the release of your chosen source. For example, if the selected source environment is release 7.0.4, the Target Environment list is populated only with other release 7.0.4 environments defined in the Configuration Manager. The association is enabled automatically when you create it.

If the environment that you want is not listed, you might need to add it. For more information, see "Adding Environment Details to the Configuration Manager" on page 3-5.

Note: Once an association is created, you cannot modify the details. You can remove an association, as described in "Deleting a Directory Association" on page 3-17.

To create an association

1. From Oracle Access Manager Configuration Manager, click the Migration tab, then the Associations:

   Migration, Associations

2. On the Association List page, click the Create New button:

   Create New

3. On the Add Association page, enter the following details to identify the source and target directories in this associated pair. For example:

   - **Association Name**: Enter a unique name that identifies this associated directory pair at a glance. For example:

     1014Dev-QA

   - **Association Description**: Enter a brief optional statement that further identifies this associated pair. For example:

     Password Policy

   - **Source Environment**: Select the name of the desired source directory from the list of existing environments. For example:

     10104DEV

   - **Target Environment**: Select the name of the desired target directory from those listed. For example:

     10104QA

4. Click Save to create the association (otherwise, click Cancel to terminate the operation).

   Save

   The Associations List page appears. The association is enabled for use automatically.

Enabling or Disabling a Directory Association

This topic explains how to disable or enable a directory association. Any individual with `HMUser` privileges can enable or disable an association. The repository for Oracle Access Manager Configuration Manager must be online. Oracle recommends that the environment (LDAP directory) also be online.

The association must be enabled for data migration. When you create a new association, it is enabled for use automatically. When an association is disabled, you cannot migrate data nor view a transaction record for the association.

You do not need to disable an association before you delete it. However, Oracle recommends that you first disable then delete the association.

To enable (or disable) a directory association

1. From Oracle Access Manager Configuration Manager, click the Migration tab, then click Associations:

   Migration, Associations

2. On the Association List page, select the option beside the desired association name. For example:

3. **Enable the Association**: On the Association List page, click the Enable button:

   Enable

   A message informs you that the association is Enabled and the Status column states "enabled".

4. **Disable the Association**: On the Association List page, click the Disable button:

   Disable

   A message informs you that the association is Disabled and the Status column states "disabled".

5. Proceed to the following topics, if needed:
   - Viewing Settings for a Directory Association
   - Creating a Directory Association
   - Deleting a Directory Association
   - Adding and Managing Optional Transformation Rules

Deleting a Directory Association

This topic explains how to delete a directory association. Any individual with `HMUser` privileges can delete an association. The repository for Oracle Access Manager Configuration Manager, and the associated LDAP directories, must be online.

Oracle recommends that you disable the association before deleting it. When you delete an association, all migration transactions related to this association are also removed. However, snapshots for a deleted association remain until you explicitly delete the snapshots.

Note: You cannot delete an environment that is part of an association. You must first delete the association and then delete the environment.

During the delete operation, you are asked to confirm that this is the action you want to take. When the association is deleted, you are returned to the Association List page where an informational message notifies you that the removal was a success.

To delete an association

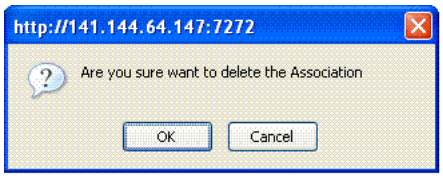
1. From Oracle Access Manager Configuration Manager, click the Migration tab, then click Associations:

   Migration, Associations

2. On the Association List page Select column, select the option beside the desired association name then click the Delete button. For example:

   Delete

   A message asks you to verify that this is what you want to do, as shown here.



3. Verify your intent to remove the association by clicking OK (or click Cancel to terminate the operation without completing it).

   OK

4. On the Association List, review the informational message that confirms that the item was deleted.
5. See related topics in this section as needed, then proceed to:
   a. About Oracle Access Manager Data
   b. Adding and Managing Optional Transformation Rules
   c. Making and Managing Snapshots
   d. Migrating Data from the Source to the Target
   e. Restarting Servers After Migration

About Oracle Access Manager Data

As mentioned in Chapter 1, certain types of data must be changed before migration to account for differences between deployments. Data that must change includes server names, IP addresses, administrative user information, and other data that is different in the new deployment. Some manual configuration or customization is necessary to ensure proper operation after migration.

The following topics give a concise overview of the objects and attributes of interest when you migrate data between deployment environments. The URLs provided in these topics can be used to validate success after data migration. For more information about each of these objects and attributes, see the *Oracle Access Manager Schema Description*:

- About Unchanged Data
- About Encryption Keys
- About Identity System Data
- About Access System Data
- About Preparing Customized Data for Manual Migration

See Also: "Adding and Managing Optional Transformation Rules" on page 3-31 and "Migrating Data from the Source to the Target" on page 3-43

About Unchanged Data

A number of objects need to be copied as is from the source to the target LDAP environment. These unchanged objects belong to the following object classes (obclass=):

- oblixOrgPerson

- oblixLocation
- oblixAuxLocation
- oblixAdvancedGroup
- oblixSiteDomain
- oblixAuthenticationPolicy
- oblixChallengeScheme
- oblixResourceOperationRule
- oblixWebResourceAuxClass
- oblixUrlPrefix
- oblixPolicyRule
- oblixWRSCAction
- oblixAuditPolicy
- oblixCustomAuthzCondition
- All object classes under obapp=WRSC
- All object classes under obname=SDSearchColumnList
- All object classes under obname=WRORSearchColumnList

About Encryption Keys

Encryption keys must be updated when you migrate across environments. These can be initially transferred as is, and modified from the Access System Console. For more information on shared secret and encryption keys, see the *Oracle Access Manager Identity and Common Administration Guide.*

The URLs provided in these topics can be used to validate success after data migration.

The following is an example LDAP URL for extracting the encryption keys:

```
ldap://server:port/obContainerId=encryptionKey,o=Oblix,ou=Apps,o=oblix.net??
sub?(o=objectclass=*)
```

The following is an example encryption key object:

```
dn: obContainerId=encryptionKey,o=Oblix,out=Apps,o=oblix.net
objectClass: oblixContainer
objectClass: top
obContainerId: encryptionKey

dn: cn=cookieEncryptionKey,obContainerId=encryptionKey,
o=Oblix,ou=Apps,o=oblix.net
cn: cookieEncryptionKey
objectClass: top
objectClass: oblixEncryptionKey
obSharedSecret:
m9+XBn7aVladIkLiJ/qfIPKjoPcS5KlpFnA7ClPECi69KXUB3EUaSU4myFYD1UmXHFJsgcC+tVBBCa9HmW
c1HumonYoCqA1cTbXwtIr8S7aEgmY7K9zGhegV6Cjwa6RGsMWYSqfIPKjoPcS5KlpFnA7ClPECi69KXUB3
EUaSU4myFYD1UmXHFJsgcC+tVBBCa9HmWc1HumonYofr1CqA1cTbXwtIr8S7aEgmY7K9zGhegV6Cjwa6RG
sMWYSYwuf9ycJYOaw==
obSecretSize: 256
```

About Identity System Data

Identity System data consists of three types of directory entries:

- Configuration data
- Run-time data
- Dynamic data, which is not migrated using Oracle Access Manager Configuration Manager

The following topics describe each data type in greater detail. The URLs provided in these topics can be used to validate success after data migration.

- Object Class Definitions
- Identity Servers
- WebPass Instances
- Directory Options
- Administrators
- Server Settings
- Auditing Policies
- Password Policies
- Workflow Configurations
- Attribute Read and Write Privileges
- Searchbases
- Workflow Tickets Cannot be Migrated using Oracle Access Manager Configuration Manager
- User, Group, and Organization Manager Panels

Object Class Definitions

Object class definitions consist of two or more objects. The first object is the top object. For instance, the following is the definition for inetOrgPerson:

```
dn: obclass=inetOrgPerson,o=Oblix,ou=Apps,ob=oblix.net
obReady: True
obVer: 7.0
obClass: inetOrgPerson
objectClass: top
objectClass: OblixClass
obClassKind: Structural
obClassType: personClass
obClassAttr: cn
```

The following is an example LDAP URL for extracting the top object:

```
ldap://server:port/o=Oblix,ou=Apps,o=oblix.net??one?(objectclass=OblixClass)
```

An object class definition consists of objects with meta-definition of the object, including its display types, semantic types, and so on. The following is an example LDAP URL for extracting the object class meta definition:

```
ldap://server:port/obClass=CLASS_
NAME,o=Oblix,ou=Apps,o=oblix.net??sub?(!(objectclass=oblixClass))
```

An example of an object class definition:

```
dn: obattr=cn,obclass=inetorgperson,o=oblix,ou=apps, o=oblix.net
obAttr: cn
obVer: 7.0.0
objectClass: top
objectClass: oblixMetaAttribute
obDisplayName: Full Name
obSemanticType: obSName
obCardinality: multi
obDisplayType; obDTextS
obSearchable: True
obVisible: True

dn: obattr=givenName,obclass=inetorgperson,o=oblix,ou=apps, o=oblix.net
obAttr: givenName
obVer: 7.0.0
objectClass: top
objectClass: oblixMetaAttribute
obDisplayName: First Name
obSemanticType: obSName
obCardinality: multi
obDisplayType; obDTextS
obSearchable: True
obVisible: True
```

The following attributes are unchanged (obpanelid=) in the Identity System:

- monitorTable
- ticketTable
- wfProfileTopPanel
- wfProfileLowerPanel
- ticketInfoTable

Identity Servers

Identity Server information is stored in the class oblixOISServerConfigInfo. The following is an example LDAP URL for extracting the Identity Server information:

```
ldap://server:port/obPolicyContainerId=WebResrcDB,obContainerId=Policies,
o=Oblix,ou=Apps,o=oblix.net??one? (objectClass=oblixOISServerConfigInfo)
```

WebPass Instances

WebPass instances consist of two or more objects:

- The first is the WebPass definition, stored in the object class oblixWebPassConfigInfo.
- The second aspect of the definitions consists of the primary and secondary failover configuration. Pointers to this information are stored in the attributes obOISPrimaryServerID and obOISSecondaryServerID. The object class oblixOISServerIDNode contains this information.

The following is an example LDAP URL for extracting the WebPass definition object:

```
ldap://server:port/obPolicyContinerId=WebResrcDB,obContainerId=Policies,
o=Oblix,ou=Apps,o=oblix.net??one? (objectClass=oblixWebpassConfigInfo)
```

The following is an example LDAP URL for extracting the WebPass primary and secondary failover information:

```
ldap://server:port/obPolicyContainerId=WebResrcDB,obContainerId=Policies,
o=Oblix,ou=Apps,o=oblix.net??one?(&(obname=OBJECT_NAME)
(objectClass=oblixOISServerIDNode))
```

where OBJECT_NAME is the WebPass identifier.

Directory Options

There are three data elements for directory options:

- Default directory server information is stored in oblixDBProfile.
- Directory profiles stored with a different obname than the default server in the oblixDBProfile object class.
- Disjoint searchbases are simple attribute values on a specific object, such as groupOfUniqueNames.

The following is an example LDAP URL for extracting the default directory server information:

```
ldap://server:port/obName=default,obContainerId=DBAgents,o=Oblix,ou=Apps,
o=oblix.net??base?(objectClass=oblixDBProfile))
```

The following is an example LDAP URL for extracting the directory profiles:

```
ldap://server:port/obName=certificateServer,obContainerId=DBAgents,o=Oblix,
ou=Apps,o=oblix.net??one?(&(objectClass=oblixDBProfile) (!obname=default)))
```

The following is an example LDAP URL for extracting the disjoint searchbases:

```
ldap://server:port/o=Oblix,ou=Apps,o=oblix.net??base?(objectClass=*)
```

Administrators

There will be directory entries for your directory administrators and Web masters.

The following is an example LDAP URL for extracting the directory administrators:

```
ldap://server:port/cn=Directory Administrators,o=Oblix,ou=Apps,o=oblix.net??base?
(objectClass=*)
```

The following is an example LDAP URL for extracting the Web Masters:

```
ldap://server:port/cn=Web
Masters,o=Oblix,ou=Apps,o=oblix.net??base?(objectClass=*)
```

Server Settings

These include settings for email feedback accounts, SMPT server settings, and session timeout values. A single object defines all of these items.

The attributes obFeedbackEmail, obWebMasterEmail, and obUserSessionTimeout are stored on this object.

The following is an example LDAP URL for extracting information for all server settings:

```
ldap://server:port/o=Oblix,ou=Apps,o=oblix.net??base?(objectClass=*)
```

Auditing Policies

Audit policies are stored in the object classes oblixMasterAuditPolicy and oblixAuditPolicy. The following is an example LDAP URL for extracting information for auditing policies:

```
ldap://server:port/obname=MasterAuditPolicy,obPolicyContainerId=WebResrcDB,
obContainerId=Policies,o=Oblix,ou=Apps,o=oblix.net??base? (objectClass=*)
```

Password Policies

Password policies are stored in the object class oblixPasswordPolicy. The following is an example LDAP URL for extracting information for password policies:

```
ldap://server:port/obContainerId=password,o=Oblix,ou=Apps,o=oblix.net??one?
(objectClass=oblixPasswordPolicy)
```

Workflow Configurations

Workflow configurations are as follows:

- Workflow definitions are stored in the object class oblixWorkflow.
- Workflow definition details are stored in the object classes oblixWorkflowTarget and oblixWorkflowStep.
- Workflow participant definitions consist of a placeholder for the participant rule, with a flag to indicate if it is enabled or disabled (in the obPolicyRuleEnabled attribute). These entries contain oblixPolicyContainerId=WorkflowDB in their DN and have attributes to link back to the workflow definition entry.
- Workflow participant condition entries store the criteria for who can participate in the workflow. These entries contain oblixPolicyContainerId=WorkflowDB in their DN.
- Workflow particpant rules: These can be one or more entries that describe what workflow the rule applies to. Each entry contains an attribute called obWorkflowName to point to the workflow definition entry for this rule. Each entry also contains an obPolicyReulName to point to the workflow participant condition entry. The object class for these rules is oblixWorkflowResourceAuxClass.

The following is an example LDAP URL for extracting information for workflow definition entries:

```
ldap://server:port/obContainerId=workflowDefinitions,o=Oblix,ou=Apps,
o=oblix.net??one?(objectClass=oblixWorkFlow)
```

The following is an example LDAP URL for extracting information for workflow definition detail entries:

```
ldap://server:port/obWorkflowId=WF_ID,obContainerId=workflowDefinitions,
o=Oblix,ou=Apps,o=oblix.net??sub?(objectClass=*)
```

where WF_ID is the value of the attribute obWorkflowId from the parent workflow definition entry.

The following is an example LDAP URL for extracting information for workflow participant definition entries:

```
ldap://server:port/obPolicyContainerId=WorkflowDB,obContainerId=Policies, o=Oblix,
ou=Apps,o=oblix.net??one? (objectClass=oblixPolicyRule)
```

The following is an example LDAP URL for extracting information for workflow participant condition entries:

```
ldap://server:port/obName=PD_ID,obPolicyContainer=WorkflowDB,
obContainerId=Policies, o=Oblix,ou=Apps,o=oblix.net??sub?
(objectClass=oblixPolicyCondition)
```

where PD_ID is the value of the obName attribute in the workflow participant definition entry.

The following is an example LDAP URL for extracting information for workflow participant operation rule entries:

```
ldap://server:port/obName=PD_ID,obPolicyContainer=WorkflowDB,
obContainerId=Policies, o=Oblix,ou=Apps,o=oblix.net??sub?(&
(objectClass=oblixResourceOperationRule) (obWorkflowName=obWorkflow=WF_ID,
obContainerId=workflowDefinitions,o=oblix,ou=Apps, o=oblix.net))
```

Attribute Read and Write Privileges

Attribute-level access control rules are stored as a number of entries in the directory.

- All attribute access controls are defined in entries with obPolicyContainerId in their DNs. The possible values for obPolicyContainerId are obGroupDB, obObjectDB, and UserDB. Example:

  ```
  dn: obname=C233409809898,obPolicyContainerId=UserDB,
  obContainerId=Policies,o=Oblix,ou=Apps,o=oblix.net
  objectClass: Top
  objectClass: oblixPolicy Rule
  obName: P222222
  obPolicyRuleConditionListType: 2
  obPolicyRuleEnabled: True
  obPolicyRulePriority: 1
  ```

- For each access control, in addition to the definition entry there is a condition entry that stores the criteria for determining who the ACL applies to. This entry contains obPolicyContainerId of obGroupDB, obObjectDB, or UserDB, and and the value of the obName attribute in the attribute access control definition entry. Example:

  ```
  dn: obname=P222222,obname=C233409809898,
  obPolicyContainerId=UserDB,obContainerId=Policies, o=Oblix,ou=Apps,o=oblix.net
  objectClass: oblixPolicyCondition
  obName: P222222
  obPolicyConditionOrder: 1
  obPolicyConditionUsage: Allow
  obPolicyConditionRole: ob_self
  ```

For each access control, there is an operation rule that define the attribute that the access control applies to. These are defined in the object class oblixResourceOperationRule.

The following is an example LDAP URL for extracting information for an ACL definition entry:

```
ldap://server:port/obPolicyContainerId=CONTAINER_TYPE,obContainerId=Policies,
o=Oblix,ou=Apps,o=oblix.net??one? (objectClass=oblixPolicyRule)
```

The CONTAINER_TYPE can be either obObjectDB, UserDB, or ObGroupDB.

The following is an example LDAP URL for extracting information for an ACL condition:

```
ldap://server:port/obName=ACL_ID,obPolicyContainerId=CONTAINER_TYPE,
obContainerId=Policies,o=Oblix,ou=Apps,o=oblix.net??sub?
(objectClass=oblixPolicyCondition)
```

The CONTAINER_TYPE can be obObjectDB, UserDB, or ObGroupDB, and ACL_ID is the value of the attribute obName in the ACL definition entry described here.

The following is an example LDAP URL for extracting information for an ACL operation rule:

```
ldap://server:port/obPolicyContainerId=CONTAINER_TYPE,obContainerId=Policies,
o=Oblix,ou=Apps,o=oblix.net??one?(& (objectClass=oblixResourceOperationRule)
(obPolicyRuleName=obName=ACL_ID, obPolicyContainerId=CONTAINER_
TYPE,obContainerId=Policies, o=Oblix,ou=Apps,o=oblix.net))
```

The CONTINER_TYPE can be obObjectDB, UserDB, or obGroupDB, and ACL_ID is the value of the attribute obName in the ACL definition entry.

Searchbases

Searchbases are defined by two types of LDAP entry:

- A single entry that serves as a high-level searchbase definition. This entry is defined using the object classes oblixResourceOperationRule and oblixUserResourceAuxClass.
- The actual searchbase conditions are stored in entries containing a DN with the value of the attribute obPolicyRuleName of the high-level searchbase definition.

The following is an example LDAP URL for extracting information for the high-level searchbase definition:

```
ldap://server:port/obPolicyContainerId=UserDB,obContainerId=Policies,o=Oblix,
ou=Apps,o=oblix.net??one?(& (objectClass=oblixResourceOperationRule)
(objectClass=oblixUserResourceAuxClass))
```

The following is an example LDAP URL for extracting the actual searchbase conditions:

```
ldap://server:port/DISTINGUISHED_NAME??sub?(objectClass=*)
```

where DISTINGUISHED_NAME is the value of the attribute obPolicyRuleName in the high-level searchbase definition.

Workflow Tickets Cannot be Migrated using Oracle Access Manager Configuration Manager

A workflow ticket *cannot* be migrated using Oracle Access Manager Configuration Manager. A workflow ticket is defined by two or more entries:

- The ticket definition created in the oblixWorkflowInstance object class.
- Additional workflow ticket data, such as attribute values and status. These entries are child entries to the ticket definition.

The following is an example LDAP URL for extracting the workflow ticket definition:

```
ldap://server:port/obContainerID=workflowInstances,o=Oblix,ou=Apps,o=oblix.net??on
e?(objectClass=oblixWorkflowInstance)
```

The following is an example LDAP URL for extracting the additional workflow ticket data:

```
ldap://server:port/obWFInstanceId=WF_
INSTANCE,obContainerId=workflowInstances,o=oblix,ou=Apps,o=oblix.net??sub?(objectC
lass=*)
```

where WF_INSTANCE is the value of the attribute obWorkflowId in the workflow ticket definition object.

> **Note:** If you are exporting and importing data using an LDIF file, workflow records must be removed from the LDIF file before you import data to the new LDAP directory environment. These records are written to the oblixWorkflowInstance object class.

User, Group, and Organization Manager Panels

These entries define the panels in the Identity applications. They are components of the obApp entries for userServCenter, groupServCenter, and objServCenter. They are identified by the following object classes:

- oblixPanel
- oblixTabPanel
- oblixLocation

Additionally, some entries can be in the oblixMetaAttribute object class with these attributes:

- obPanelType
- obLocationName
- obLocationTitle
- obPanelID
- obParentLocationDN
- obRectangle
- obPhoto

User Manager Example

The following is an example LDAP URL for extracting the information on User Manager panels:

```
ldap://server:host/obApp=userServCenter,o=Oblix,ou=Apps,o=oblixl.net??sub?
(objectClass=*)
```

Group Manager Example

The following is an example LDAP URL for extracting the information on Group Manager panels:

```
ldap://server:host/obApp=groupServCenter,o=Oblix,ou=Apps,o=oblixl.net??sub?
(objectClass=*)
```

Organization Manager Example

The following is an example LDAP URL for extracting the information on Organization Manager panels:

```
ldap://server:host/obApp=objServCenter,o=Oblix,ou=Apps,o=oblixl.net??sub?
(objectClass=*)
```

About Access System Data

Access System LDAP entries that can be migrated using Oracle Access Manager Configuration Manager are categorized and described in the following topics. The URLs provided in these topics can be used to validate success after data migration. Topics here include:

- Master Web Resource Administrators
- Resource Type Definitions
- Host Identifiers
- Access Servers
- Access Clients
- Authentication and Authorization Schemes
- Auditing Policies
- Cache Update Requests Cannot be Migrated using Oracle Access Manager Configuration Manager
- Policy Domains

Master Web Resource Administrators

These entries describe the Access Administrators. Example:

```
dn: cn=Master Web Resource Admins,obapp=PSC,o=Oblix, ou=apps,o=oblix.net
objectClass: groupOfUniqueNames
objectClass: top
objectClass: oblixGroupOfUniqueNames
obUniqueMember: uid=jdoe,ou=People,o=oblix.net
obVer: 7.0
cn: Master Access Administrator
```

The following is an example LDAP URL for extracting the information on Master Web Resource Administrators:

```
ldap://server:port/cn=Master Web Resource
Admins,obApp=PSC,o=Oblix,ou=Apps,o=oblix.net??base? (objectClass=*)
```

Resource Type Definitions

These entries belong to the object class oblixResourceType. The following is an example LDAP URL for extracting the information on resource type definitions:

```
ldap://server:port/obContainerId=URI
Resources,obApp=PSC,o=Oblix,ou=apps,o=oblix.net??one?
(objectClass=oblixResourceType)
```

Host Identifiers

These entries belong to the object class oblixHostId. The following is an example LDAP URL for extracting the information on host identifiers:

```
ldap://server:port/obapp=PSC,o=Oblix,ou=apps,o=oblix.net??one?
(objectClass=oblixHostId)
```

Access Servers

These entries belong to the object classes oblixAAAServerConfigInfo and oblixAAAEngineConfig. The following is an example LDAP URL for extracting the information on Access Servers:

```
ldap://server:port/obApp=PSC,o=Oblix,ou=apps,o=oblix.net??one?(&
(objectClass=oblixAAAServerConfigInfo) (objectClass=oblixAAAEngineConfig))
```

Access Clients

Access clients consist of two or more objects:

- The actual AccessGate, defined by the object class oblixWebgateConfigInfo.
- Primary and secondary failover information. The attributes obAAAPrimaryServerId and obAAASecondaryServerid in the Access client definitions will point at these objects. They will belong to the oblixAAAServerIDNode object class.

The following is an example LDAP URL for extracting the information on the Access Client definition object:

```
ldap://server:port/obApp=PSC,o=Oblix,ou=apps,o=oblix.net??one?
(objectClass=oblixWebGateConfigInfo)
```

The following is an example LDAP URL for extracting the information on the primary and secondary failover configuration:

```
ldap://server:port/obApp=PSC,o=Oblix,ou=Apps,o=oblix.net??one?(& (obName=OBJECT_
NAME)(objectClass=oblixAAAServerIDNode))
```

where OBJECT_NAME is any name that corresponds to the primary and secondary server IDs.

Authentication and Authorization Schemes

These belong to the oblixChallengeScheme object class. The following is an example LDAP URL for extracting the information on authentication schemes:

```
ldap://server:port/obApp=PSC,o=Oblix,ou=apps,o=oblix.net??one?
(objectClass=OblixChallengeScheme)
```

The following is an example LDAP URL for extracting the information on authorization schemes:

```
ldap://server:port/obApp=PSC,o=Oblix,ou=apps,o=oblix.net??one?
(objectClass=OblixAuthzPluginScheme)
```

Auditing Policies

These belong to the oblixAuditPolicy and oblixMasterAuditPolicy object classes.

The following is an example LDAP URL for extracting the information on auditing policies:

```
ldap://server:port/obApp=PSC,o=Oblix,ou=apps,o=oblix.net??one?(&
(objectClass=oblixAuditPolicy) (objectClass=oblixMasterAuditPolicy))
```

Cache Update Requests Cannot be Migrated using Oracle Access Manager Configuration Manager

These belong to the oblixGSN object class. Cache update requests cannot be migrated using Oracle Access Manager Configuration Manager.

If you choose to migrate these manually, cache update messages should not be synchronized, except for the last sequence number. There are two objects that should be considered when migrating:

- The last cache update sent in the system is stored on a special object, but it needs to have a shadow record with the description of the update. This record is in the oblixSynchRecord object class.
- The individual cache update notification message created as an entry of the oblixSynchRecord object class

The following is an example LDAP URL for extracting the information on the last cache update:

```
ldap://server:port/obApp=PSC,o=Oblix,ou=apps,o=oblix.net??one?
(objectClass=oblixGSN)
```

The following is an example LDAP URL for extracting the information on the cache update notification message:

```
ldap://server:port/cn=PSCMgmt,obApp=PSC,o=Oblix.ou=apps,o=oblix.net??one?(&
(obSyncRequestNo=*)(objectClass=oblixSynchRecord))
```

Policy Domains

Policy Domains consist of multiple objects organized in a single two-level LDAP branch where the policy domain definition is the top of the branch, and the child objects define the behavior of the policy domain. These objects belong to the oblixSiteDomain object class.

The following is an example LDAP URL for extracting the information on the policy domain:

```
ldap://server:port/obApp=PSC,o=Oblix,ou=apps,o=oblix.net??one?
(objectClass=oblixSiteDomain)
```

For each policy domain, the following rule outputs the elements that make up the domain:

```
ldap://server:port/obName=SITE_DOMAIN_NAME,obApp=PSC,o=Oblix,ou=apps,
o=oblix.net??sub?(objectClass=*)
```

where SITE_DOMAIN_NAME is the value of the attribute obName that serves as the unique identifier for the policy domain parent object.

About Preparing Customized Data for Manual Migration

Oracle Access Manager Configuration Manager does not automate data migration for all types of data. Customized data must be migrated from a source deployment to a target deployment manually. Table 3–4 outlines the types of Identity System data that are *not* supported for migration using Oracle Access Manager Configuration Manager.

Table 3–4 Identity System Data to Migrate Manually

Identity System Data for Manual Migration
PPP Catalog (and associated called scripts/code)
Javascripts
Images
Stylesheets

Table 3–5 outlines the Access System data types that are *not* supported for migration using Oracle Access Manager Configuration Manager.

Table 3–5 Access System Data to Migrate Manually

Access System Data to Migrate Manually
Authentication Plug-in Code
Authorization Plug-in Code

To migrate data listed in Table 3–4 and Table 3–5, you can have (or know of) other code management products that can be used for check in, check out, and deployment. Details of third-party products is outside the scope of this manual.

Standard Oracle recommendations that are of particular importance when preparing to migrate customized Oracle Access Manager data include:

- Standardizing the layout of the file system in all of the LDAP directory environments in each deployment.

  Oracle recommends that you locate all Oracle Access Manager-specific files in one directory path across all environments.

- Ensuring that Web server and directory server versions are the same across all environments.

- Creating a `customizations` directory where you store all custom code.

  Your `customizations` directory should not be in the installation directory of the Oracle Access Manager component. When reinstalling or uninstalling an Oracle Access Manager component, all subdirectories are deleted.

- Documenting your changes and customizations.

Specific recommendations for migrating customizations to another deployment are explained in the following topics:

- Recommendations for JavaScript files
- Recommendations for Identity Event API (PPP) hooks
- Recommendations for XSL stylesheets

Recommendations for JavaScript files

- Avoid modifying the main misc.js and miscsc.js files located in the WebPass directory.

  These files are used for client-side processing and are common to all Oracle Access Manager components. Any modification can adversely affect all components. If you do modify these files, and you are migrating across environments, remember that the XSL stylesheets include these files. When migrating across environments, you need to modify the newer versions of the files to reflect the changes made to the existing files.

- Create a separate stylesheet that incorporates all of the JavaScript hooks and include that stylesheet in other affected stylesheets.
- Document your changes.

Recommendations for Identity Event API (PPP) hooks

- Be sure that you are running the same version of the development software in all deployments. For example, if you are using a Java or PERL executable, make sure that the versions of the PERL interpreter and JVM are the same. This is also true for C compilers.
- You cannot migrate oblixpppcatalog.lst because it contains references to specific workflow IDs that might or might not be present in the new environment.
- Document the changes.

Recommendations for XSL stylesheets

- Create a separate instance of the stylesheets before modifying anything.

  To do this, define a new stylesheet that contains all of your new styles.

- If you are modifying the client-side images, styles, and so on, all of these changes must go into all of the affected WebPass instances.

For more information, see the *Oracle Access Manager Customization Guide*.

Adding and Managing Optional Transformation Rules

As discussed in Chapter 1, you have the following options for applying changes to logical object attributes:

- After creating an association, you can create optional transformation rules that will be applied during the migration operation using the procedure in this section.
- During the migration operation, transformation rules are applied and the results are presented to you. You can then customize attributes manually as described in "Migrating Data" on page 3-51.
- After migration, you can change attribute values as follows:
  - On the Rollback Transaction, Customize page. For more information, see "Rolling Back Changes Made During a Specific Transaction" on page 5-3.
  - Directly in the target Oracle Access Manager 10*g* (10.1.4.0.1), or Oracle COREid Release 7.0.4, deployment using the System Console. For more information, see the product administration guide for the specific release of your deployment as described in "Related Documents" on page x.

A **transformation rule** is one that you define for a specific directory association before you start migrating data. Transformation rules are applied during the customization

phase of the migration operation. Each transformation rule converts existing logical object attribute values and system-specific settings to a value that you specify when you define the rule. On the Customize page, you can see the logical object as it is before the rule is applied *(Before Migration)* and as it will be after the rule is applied *(After Migration)*.

For example, suppose that you are migrating 20 password policies and you want to change the `Number of login tries allowed` attribute value from `2` to `3` (or you want to change `Hostname` variations while migrating Host identifiers). You can create a transformation rule before data migration that be applied and perform these activities during data migration.

Any individual with `HMUser` privileges can perform tasks related to transformation rules. The repository for Oracle Access Manager Configuration Manager and the associated LDAP directories must be online while you perform these tasks.

Confirm that the prerequisite tasks outlined in Table 3–6 are completed before you start defining optional transformation rules.

Table 3–6 Transformation Rule Prerequisites

Confirm	Prerequisite Tasks	Look in
	Add environment details for at least two LDAP directories within deployments of the same release.	Adding Environment Details to the Configuration Manager on page 3-5
	Create at least one directory association to specify the source and target environments for your transformation rule.	Creating a Directory Association on page 3-15

Task overview: Adding and managing transformation rules includes

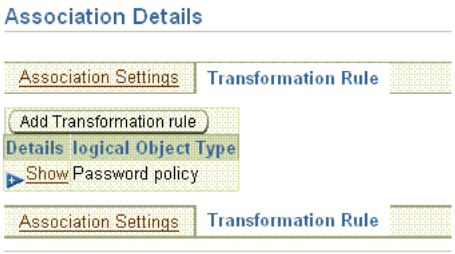
1. Viewing Transformation Rules
2. Adding an Optional Transformation Rule
3. Modifying a Transformation Rule
4. Deleting a Transformation Rule

Viewing Transformation Rules

You use the procedure in this topic to view an existing transformation rule for a directory association. Any individual with `HMUser` privileges can perform this task. The repository for Oracle Access Manager Configuration Manager and the associated LDAP directories must be online while you perform these tasks.

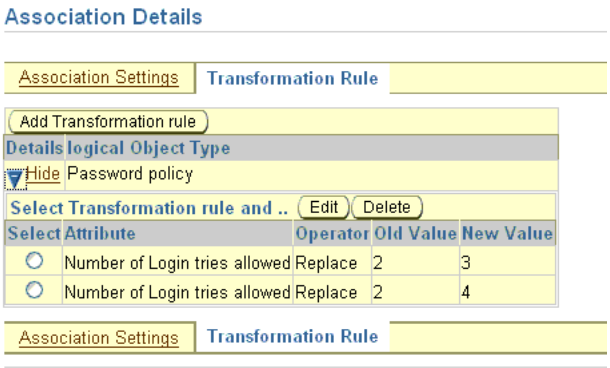
When you click the Associations secondary tab under the Migrate tab, the Association List page appears. After selecting a name in the Association Name column to display the Association Details page, you click the Transformation Rules subtab. Details about existing transformation rules for the association appear in a table as shown in Figure 3–8. Initially, the Transformation Rule table displays only the logical object types on the target for which a transformation rule exists. If no rule exists, a message states "No Transformation Rules were found".

Figure 3–8 Transformation Rules Page and Table



You click the Show arrow beside the desired logical object type to expand details. Figure 3–9 shows the types of details outlined for the transformation rule, which include Attribute, Operator, Old Value, and New Value. The Edit, Delete, and Add Transformation Rule buttons are also available.

Figure 3–9 Rule Details with Edit, Delete, and Add Transformation Rule Buttons



To view a transformation rule

1. From Oracle Access Manager Configuration Manager, click the Migration tab, then click Associations:

   Migration, Associations

2. In the Association Name column, click the desired name. For example:

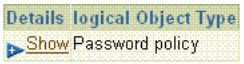
   

   The Association Details page appears.

3. On the Association Details page, click the Transformation Rule subtab. For example:

4. Click the Show arrow beside the desired logical object type to display the corresponding rules and attributes. For example:



5. Proceed to the following topics if desired:
   - Adding an Optional Transformation Rule
   - Modifying a Transformation Rule
   - Deleting a Transformation Rule

Adding an Optional Transformation Rule

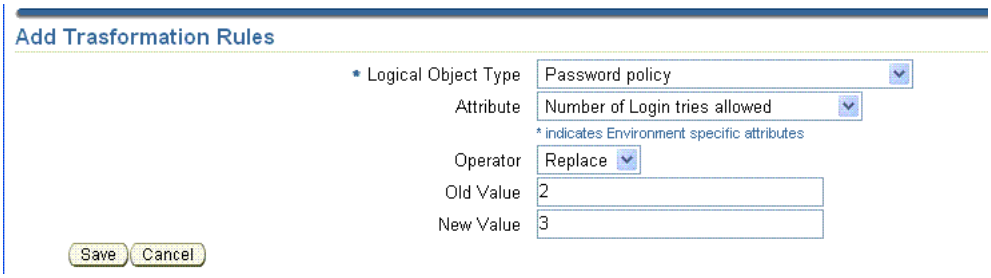
You use the procedure in this topic to add an optional transformation rule for a directory association that will automatically change an attribute value on the target during data migration. Any individual with `HMUser` privileges can perform this task. The repository for Oracle Access Manager Configuration Manager and the associated LDAP directories must be online while you perform these tasks.

You start this operation much the same as you would when viewing a transformation rule. For example, you select an existing association name and then click the Transformation Rule subtab. If the desired association is not listed, ensure that it was formed as described in "Creating a Directory Association" on page 3-15.

From the Transformation Rule subtab, you click the Add Transformation Rule button. On the Add Transformation Rule page, lists are initially empty and fields are blank. The available attributes depend on the logical object type you select. The available operators depend upon the attribute you select. In the Attribute list, system-specific attributes are shown with an asterisk, *.

You select a logical object type and a related attribute to which the rule will be applied. You then select an operator. To finish, you enter the old parameter value and a new parameter value as described in the following procedure. A completed transformation rule will look like the example in Figure 3–10.

Figure 3–10 Add Transformation Rule Page



To add a transformation rule to a directory association

1. From Oracle Access Manager Configuration Manager, click the Migration tab, then click Associations. For example:

   Migration, Associations

2. In the Association Name column, click the desired name. For example:

The Association Details page appears.

3. Click the Transformation Rules subtab. For example:

   Transformation Rules

   The Transformation Rules page appears with the Add Transformation Rule button. Included is a table of logical object types for which rules are defined within this association. The table is empty if no rules are defined for this association.

4. Click the Add Transformation Rule button to display the page where you can create a new rule.

   Add Transformation Rule

   The Add Transformation Rules page provides lists from which you select specific elements of the rule and a field where you enter a specific parameter for this rule.

5. On the Add Transformation Rules page, select from the lists to define this rule. For example:

   - **Logical Object Type**: Select the appropriate logical object type from the list. For example:

     Password Policy

   - **Attribute**: Select the desired attribute from the list, which varies depending upon the selected logical object type. For example:

     Number of Login Tries Allowed

   - **Operator**: Select the appropriate operator for this attribute and rule. For example:

     Replace

   - **Old Value**: Enter the old value of the parameter. For example:

     2

   - **New Value**: Enter the new value of the parameter. For example:

     3

6. Click the Save button to complete the operation (or Cancel to terminate without saving this rule).

   Save

   The Association Details page appears with a message announcing that your transformation rule has been saved.

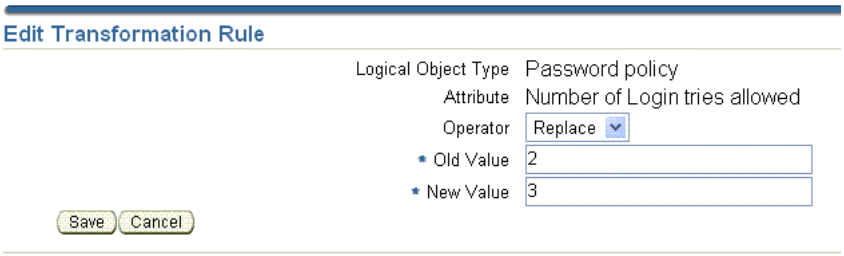
7. Click the Transformation Rule subtab to add other transformation rules or to modify or delete a transformation rule.

Modifying a Transformation Rule

Any individual with `HMUser` privileges can perform this task. The repository for Oracle Access Manager Configuration Manager and the associated LDAP directories must be online while you perform these tasks.

You use the procedure here to edit an existing transformation rule for an association. For example, you can use this procedure to make a correction using the page shown in Figure 3–11.

Figure 3–11 Edit Transformation Rule Page



This procedure is similar to creating a transformation rule. However when you edit a rule, the Logical Object Type and Attribute are fixed and cannot be changed. Only the operator list, and the old and new value fields are active and can be used to modify current information.

To edit a transformation rule

1. From Oracle Access Manager Configuration Manager, click the Migration tab, then click Associations. For example:

   Migration, Associations

2. In the Association Name column, click the desired name. For example:

   The Association Details page appears.

3. Click the Transformation Rules subtab to display the Transformation Rules page. For example:

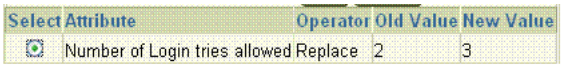
   Transformation Rules

   The Transformation Rules page organizes logical object types for which rules have been created in a table.

4. Click the Show arrow beside the desired logical object type to display details about this rule. For example:

   Show

5. Select the attribute option to edit. For example:

6. Click the Edit button to display the page where you can modify this rule.

   Edit

7. Modify the details for this transformation rule using the guidelines in "Adding an Optional Transformation Rule" on page 3-34.

8. Click Save to retain this change (or Cancel to terminate the operation).

   Save

9. Repeat this procedure to modify other transformation rules or proceed to following related topics as needed:

- Adding an Optional Transformation Rule
- Deleting a Transformation Rule

Deleting a Transformation Rule

You use the procedure in this topic to remove an existing transformation rule from the association. Any individual with `HMUser` privileges can perform this task. The repository for Oracle Access Manager Configuration Manager and the associated LDAP directories must be online while you perform these tasks.

The delete operation cannot be undone. Before the rule is deleted, a message asks you to verify that this is the action you want to take. After the transformation rule is deleted, an informational message notifies you that the operation was a success. You cannot restore a deleted transformation rule; instead, you must re-create itd.

To delete a transformation rule

1. From Oracle Access Manager Configuration Manager, click the Migration tab, then click Associations. For example:

   Migration, Associations

2. In the Association Name column, click the desired name. For example:

   The Association Details page appears containing both the current Association Settings and the Transformation Rules subtab.

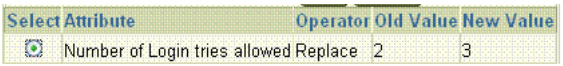
3. On the Association Details page, click the Transformation Rules subtab.

   Transformation Rules

4. Click the Show arrow to display the desired rule. For example:

   Show

5. On the Transformation Rules page, select the option beside the desired attribute to delete. For example:

6. Click the Delete button to remove this rule. For example:

   Delete

   A message asks you to verify this operation.

7. Verify by clicking OK in the message window (or click Cancel to terminate the operation without completing it). For example:

   OK

8. Review the informational message and confirm that the item no longer appears in the rules table.
9. Repeat as needed to remove other rules.
10. Proceed to the following sections before migrating data:
    - Making and Managing Snapshots

- Migrating Data from the Source to the Target

Making and Managing Snapshots

Oracle Access Manager Configuration Manager provides a SnapShot function that enables you to create a backup copy of the entire `oblix` tree in a selected environment (LDAP directory defined in the Configuration Manager). You can restore a snapshot to restore the entire `oblix` tree to the directory.

Making a snapshot does not significantly impact performance of the directory nor Oracle Access Manager Configuration Manager performance.

Confirm that all prerequisite tasks in Table 3–7 have been performed before making a snapshot.

Table 3–7 Snapshot Prerequisites

Confirm	Prerequisite Tasks	Look in
	Add environment details in the Configuration Manager	Adding Environment Details to the Configuration Manager on page 3-5
	Notify administrators of the snapshot window in advance	Notifying Other Administrators on page 3-3
	Confirm that the appropriate environment is accessible to the Configuration Manager	Testing the Environment Connection on page 3-12

Any individual with `HMUser` privileges can perform the tasks outlined in the following overview. The repository for Oracle Access Manager Configuration Manager and the associated LDAP directories must be online while you perform these tasks.

Task overview: Making and managing snapshots

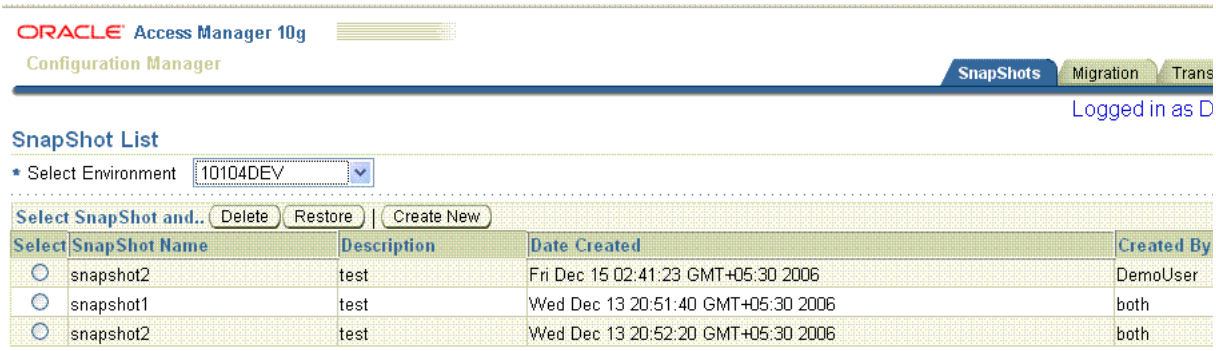
1. Viewing the SnapShot List
2. Creating a Snapshot
3. Deleting a Snapshot
4. Restoring the Content of a Snapshot

Viewing the SnapShot List

You can view some information about a snapshot made using Oracle Access Manager Configuration Manager. However, you *cannot* view the actual content of a snapshot. Any individual with `HMUser` privileges can perform this task. The repository for Oracle Access Manager Configuration Manager and LDAP directory environment must be online.

You start from the SnapShots tab and select an environment name from the Select Environment list. The table is empty until you select an environment. If snapshots exist for this environment, details are organized in a table as shown in Figure 3–12. Details that you can view include the snapshot name, an optional description, the date the snapshot was created, and the individual who created the snapshot. The table is empty if no snapshots exist for this environment.

Figure 3–12 SnapShot List Page with Details



You can view snapshot details using the following procedure However, you cannot view the content of a snapshot.

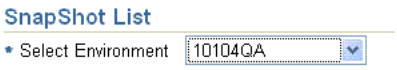
To view snapshot details

1. From Oracle Access Manager Configuration Manager, click the SnapShots tab. For example:

   SnapShots

   The SnapShots List page appears. At this point, you can either select an environment or create a new snapshot.

2. From the Select Environments list, choose an environment. For example:



   If snapshots exist for the selected environment, details are organized in a table. Otherwise, a message in the table informs you that no items were found.

3. Proceed to the following topics, as needed:

   - Creating a Snapshot
   - Deleting a Snapshot
   - Restoring the Content of a Snapshot

Creating a Snapshot

You use the following procedure to create a snapshot of an existing environment. Any individual with `HMUser` privileges can perform this task. The repository for Oracle Access Manager Configuration Manager and the LDAP directory environment must be online.

The snapshot can be used *only* by Oracle Access Manager Configuration Manager. If you are migrating configuration data using the Configuration Manager, Oracle recommends that make a snapshot of the target just before migrating data. If you are using the Configuration Manager to export configuration data to an LDIF file, Oracle recommends that you create a snapshot of the target just before *importing* the LDIF file.

There is no significant affect the LDAP directory nor Configuration Manager performance during the snapshot process. The duration of the snapshot process

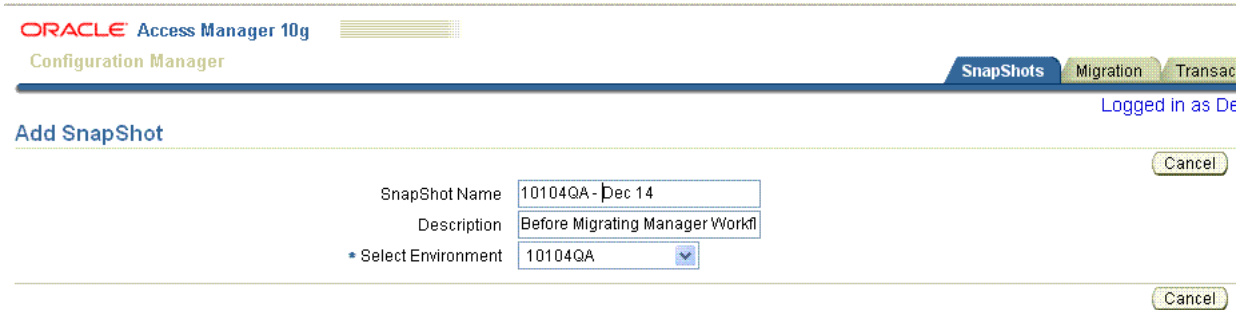
depends on the amount of configuration data in the `oblix` tree in the selected environment.

> **Note:** Oracle recommends that you schedule a window of time for this operation and notify other administrators before starting. For more information, see "Notifying Other Administrators" on page 3-3.

From the SnapShots tab you select an environment from the list, and then click the Create New button to display the Add SnapShot page. You enter the snapshot name and optional description in the fields provided.

When naming a snapshot or adding a description, you can use any combination of upper and lower case alpha/numeric characters, as well as spaces and punctuation. You then select an environment from the Select Environment list. A completed Add SnapShot page is shown in Figure 3–13.

Figure 3–13 Add SnapShot Page



When you click the Save button, the snapshot is created. When the process completes, an informational message confirms that the operation was successful. The new snapshot name and details appear in the table on the SnapShot List page. You cannot view the actual content of a snapshot.

To create a snapshot

1. From Oracle Access Manager Configuration Manager, click the Snapshots tab. For example:

   SnapShots

2. Select an environment from the Select Environments list. For example:

3. Click the Create New button to display the Add Snapshot page.

   Create New

4. Fill in the Add SnapShot page with information appropriate to your environment, as follows:

   - **SnapShot Name**: Enter a unique name that will identify this specific snapshot in the list. For example:

     10104QA - Dec 14

- **Description**: Enter an optional description to further distinguish this from other snapshots in the list. For example:

  ```
  Before migrating Manager Workflow
  ```

- **Select Environment**: From the list, select the specific directory for which you want to capture a snapshot. For example:

  ```
  10104QA
  ```

5. Select Save to assign this information and create the snapshot (otherwise select Cancel to terminate the operation without creating the snapshot).

   Save

   When the operation completes, you are returned to the Snapshot List page where you should see a message confirming that the Snapshot was saved.

6. Check the message and the table to confirm that the snapshot is available for possible restoration later.

   - **Snapshot Successful**: Proceed with migration.
   - **Snapshot Not Successful**: If you receive an error message, test the connection to the environment and the repository to ensure that these are live and online.

Deleting a Snapshot

You use the following procedure to delete a snapshot. Any individual with `HMUser` privileges can perform this task. The repository for Oracle Access Manager Configuration Manager and the LDAP environment must be online.

Note: Deleting a snapshot cannot be undone. Once a snapshot is deleted, you *cannot* use it for any restoration operation.

Deleting a snapshot cannot be undone. During this procedure, a message asks you to verify that you do want to delete the snapshot. When you confirm, the operation completes and you are returned to the SnapShots List page. An informational message notifies you that the snapshot was deleted; related details are removed from the table.

To delete a snapshot

1. From Oracle Access Manager Configuration Manager, click the SnapShots tab:

   SnapShots

2. Select an environment from the Select Environments list. For example:

3. In the Select column, click the option beside the name of the snapshot you want to delete. For example:

4. Click the Delete button.

Delete

A message asks you to verify that you want to delete the snapshot.

5. Click OK in the message window to verify removing the snapshot (otherwise, click Cancel to terminate the operation).

   OK

6. On the SnapShots List page, review the informational message and validate that the selected item was deleted.

Restoring the Content of a Snapshot

You might want to restore a snapshot if configuration data in the `oblix` tree of the environment becomes inconsistent or is corrupted as a result of changes that are external to Oracle Access Manager Configuration Manager. Any individual with `HMUser` privileges can perform this task. The repository for Oracle Access Manager Configuration Manager and the appropriate LDAP directory environment must be online.

When you restore a snapshot that was made using Oracle Access Manager Configuration Manager, the entire `oblix` tree is restored to the directory. Changes that are undone when you restore the snapshot include both migration changes that were made using the Configuration Manager, as well as changes that were made outside the Configuration Manager after data migration.

Caution: Restoring a snapshot will undo all changes made after the snapshot was taken and returns the directory to the state it was in at the time the snapshot was made.

Before the restoration commences, you are asked to verify that you want to restore the selected snapshot. After your verification, a new snapshot is created to capture the current state of the directory, and then the selected earlier snapshot is restored. If you believe that too many changes were undone during the restoration, you can restore the snapshot that was made during the restoration.

Note: If you created a directory backup using any application other than Oracle Access Manager Configuration Manager, you cannot use the Configuration Manager to restore the backup.

To restore the content of a snapshot

1. From Oracle Access Manager Configuration Manager, click the SnapShots tab. For example:

   SnapShots

2. Select an environment from the Select Environment list. For example:

3. In the Select column, click the option beside the name of the snapshot that you want to restore. For example:

4. Click the Restore button. For example:

   Restore

   A message asks you to verify that you want to complete the Restore operation, which returns the `oblix` tree in the environment to its previous condition.

5. Click OK to complete the restoration (or Cancel to terminate the operation).

   OK

   After you verify the operation, a new snapshot is made of the environment in its current state, and then the content of the selected snapshot is restored.

6. On the SnapShots List, review the informational message to confirm success; you should see the new snapshot details in the table.

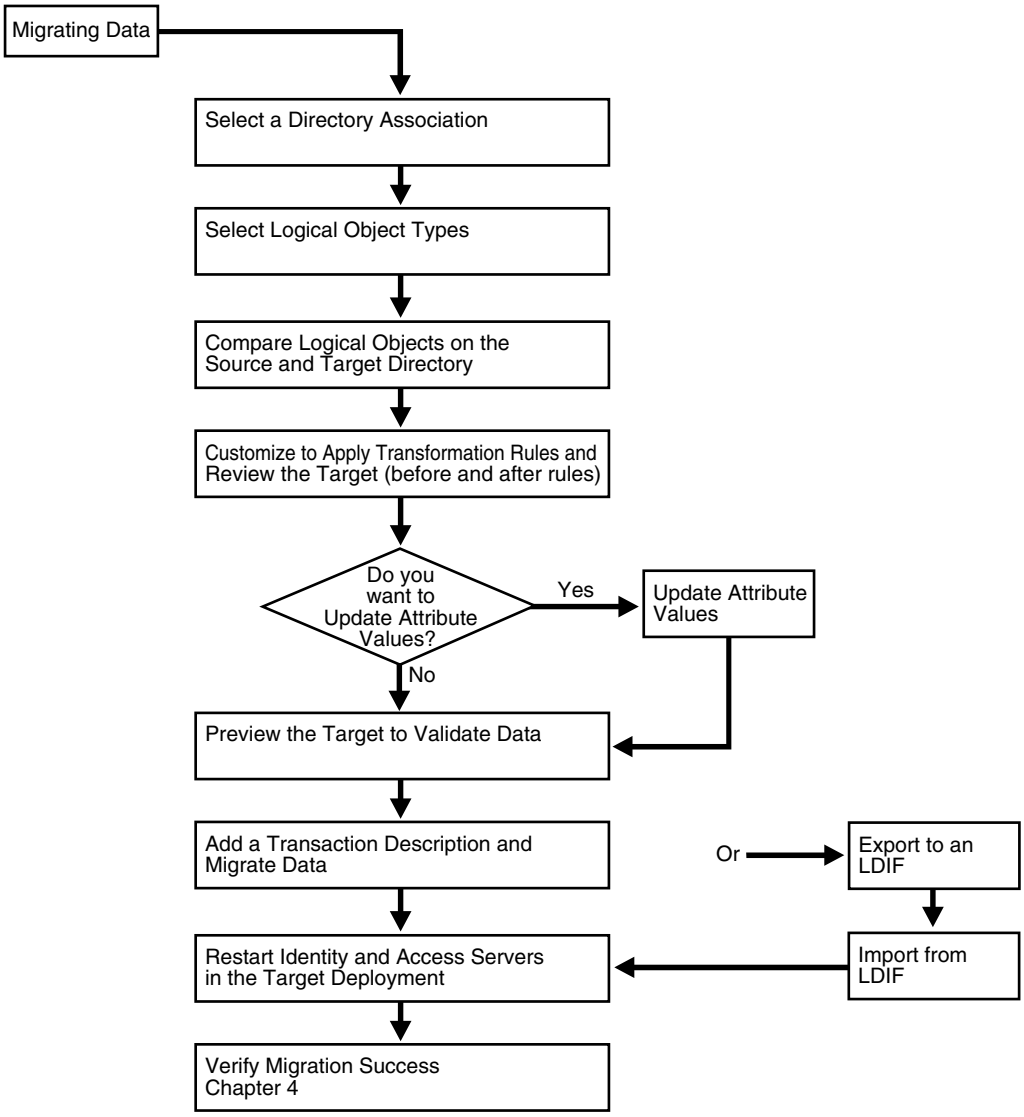
Migrating Data from the Source to the Target

Topics here include migration overviews that explain the migration process and all activities you will perform. Following the overviews is a step-by-step procedure to guide you. Any individual with `HMUser` privileges can perform this task. The repository for Oracle Access Manager Configuration Manager and the associated LDAP directories must be online during all migration activities.

Note: Oracle recommends that you schedule a migration window and notify administrators before migrating data. For more information, see "Notifying Other Administrators" on page 3-3.

Figure 3–14 illustrates the migration process and tasks that you will perform using the Configuration Manager. Additional details follow the figure.

Figure 3–14 Migration Task, Step by Step



The following task overview presumes that you have completed all prerequisite tasks in Table 3–8 on page 3-51.

Task overview: Migrating data after selecting the Migration tab, and Migrate subtab

1. You select a directory association to specify the migration path: This is required and described in "About Selecting an Association" on page 3-45.
2. You select logical object (logical object types) to migrate: This is required and is introduced in "About Selecting Logical Objects to Migrate" on page 3-46.
3. You compare the logical objects that you selected in a navigation tree:
   - To review the differences on the source and the target
   - To see related objects that you can select and migrate, as well as dependents that will be migrated automatically

For more information, see "About Comparing Data Before Migration" on page 3-46.

4. You can choose to customize the selected logical objects:
   - **Automated Method**: To automatically apply any optional transformation rules that were defined for this association. For more information, see "Adding and Managing Optional Transformation Rules" on page 3-31.
   - **Manual Method**: Edit logical object attributes manually to assign new values that will be applied to the target during migration. For more information, see "About Customizing the Target" on page 3-48
5. You preview the target system to review the selected logical objects as they are now and as they will be when migration completes. For more information, see "About Previewing Before Migration" on page 3-50.
6. You enter a unique transaction description to identity the record of this migration, which is created automatically, then migrate the data. For more information, see "Migrating Data" on page 3-51.

   Alternative: Export data to an LDIF file, then import the data offline (using an external tool to import the data). For more information, see "About Exporting Data to an LDIF File (Optional)" on page 3-50.
7. You restart all Identity Servers and Access Servers in the target environment, as described in "Restarting Servers After Migration" on page 3-55.

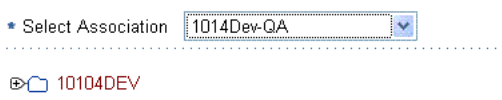
Caution: You *cannot* use Oracle Access Manager Configuration Manager to migrate data between environments that are a different release. Oracle Access Manager Configuration Manager performs checks to ensure this does not occur. For more information, see "Deployment Support and Interoperability" on page 1-16.

About Selecting an Association

This topic introduces requirements to display logical object types so you can select them for migration. Step-by-step instructions are provided in "Migrating Data" on page 3-51.

The LDAP directory environments that you will use during the migration must be online and accessible to the Configuration Manager. You start the data migration procedure by clicking the Migration tab, then the Migrate secondary tab. The Select Logical Objects to Compare page appears. A progress indicator appears at the top of the page: Select is highlighted. From here, you must select an association to specify the migration path from a source environment to a target environment, as shown in Figure 3–15.

Figure 3–15 Association Name, Select Logical Objects to Compare Page



You are ready to select logical object types, as described next.

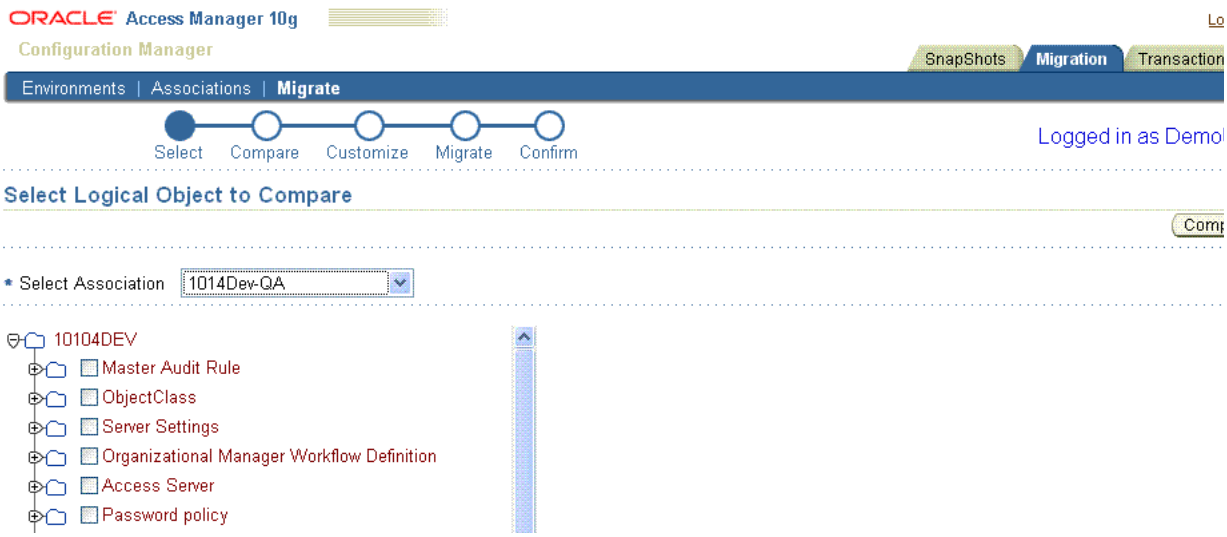
About Selecting Logical Objects to Migrate

This topic introduces the method that you use to select logical object types for migration. Step-by-step instructions are provided in "Migrating Data" on page 3-51.

After you select an association, a folder appears representing the source environment. You can select the expansion icon to the left of the icon to display logical object types on the source. A scroll bar beside the list enables you to scroll up and down as needed.

When you click the expansion icon beside the folder, all supported logical object types in the environment are displayed, as shown in Figure 3–16. A check box beside each logical object type enables you to select (or clear) items to compare. No defaults are selected.

Figure 3–16 Partial Logical Object Types List



Each logical object folder includes an expansion icon. When you expand a logical object type, you can see the logical objects grouped under that type. You can select as many logical object types (or logical objects) as needed:

- Select the check box beside a logical object type to compare all logical objects of a particular type.
- Click the expansion icon beside a folder to expand the type and display logical objects.

After selecting logical object types (or logical objects), your next activity is to compare the selected logical object types as described next.

About Comparing Data Before Migration

This topic introduces the method that you use to view and compare differences between logical objects on the source and target at one time. Step-by-step instructions are provided in "Migrating Data" on page 3-51.

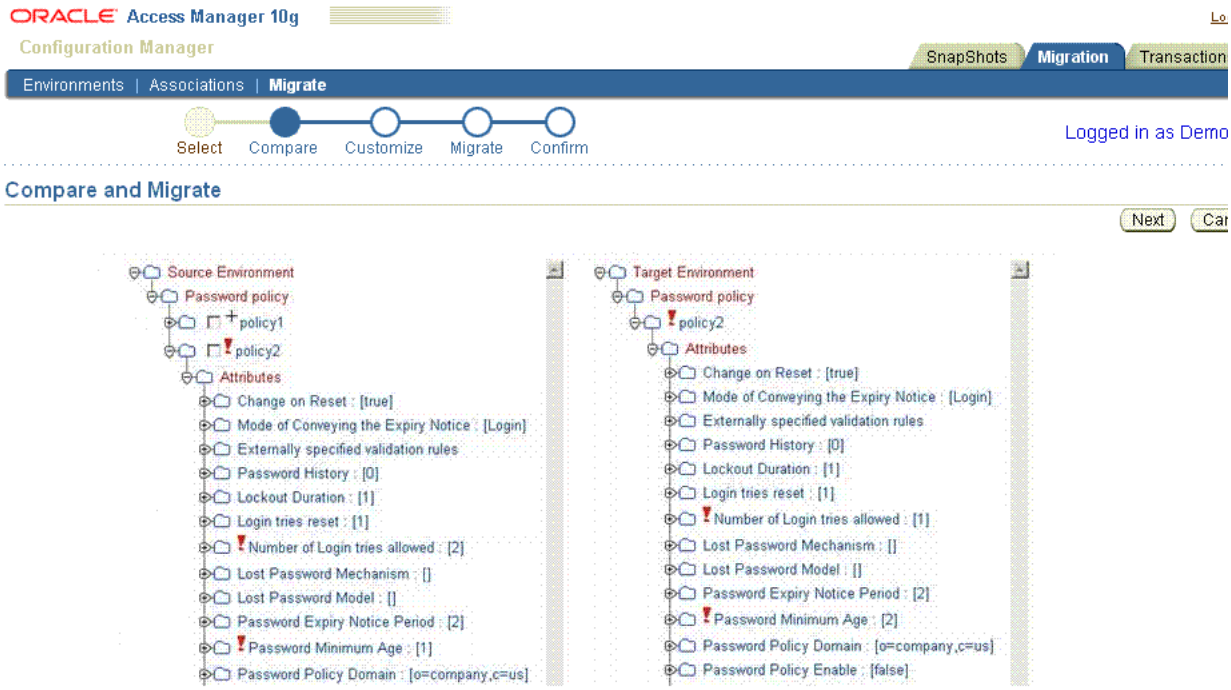
After you select items on the Select Logical Object Types to Compare page and click the Compare button, the Compare and Migrate page appears.
Both the source and target environments are shown. In the progress indicator, Compare is highlighted. Scroll bars are available on both the page and browser window.

When you click either title, Source Environment or Target Environment, details about both environments expand into a navigation tree. Expanded information is based on the logical object types (or logical objects) that you selected.

Expanding Objects to Compare: Initially, folders for the source and target environment are collapsed. You click the icon to the left of a folder to expand or collapse the navigation tree for the object.

Expanding an object in one view results in an expansion of the object in both views. Expanded objects show attributes, related objects, and dependents. For more information about related objects and dependents, see "Physical Entries and Logical Objects" on page 1-7. A sample Compare and Migrate page is shown in Figure 3–17.

Figure 3–17 Partial Compare and Migrate Page



Only Differences Are Displayed: Whether you select logical object types or specific logical objects, the Compare and Migrate page shows only the differences between the source and target. For example, suppose that you have five workflows: WF1, WF2, WF3, WF4, and WF5 in the source environment and suppose that:

- WF1 is also present in the target with a different Description attribute
- WF2 and WF3 are *not* in the target environment
- WF4 and WF5 are the *same* in the source and the target environments

If you selected only the *logical object type* User Manager Workflow Definition, the Compare and Migrate page will display WF1 (because it has a different Description attribute) along with WF2 and WF3 which are not yet on the target.

However, if you selected *logical objects* WF1, WF2, WF4, the Compare and Migrate page shows WF1 (because it has a different attribute value), and WF2 (because it does not exist on the target at this time). However, WF4 is *not* shown because it is the same in both the source and target environments.

Symbols Highlight Differences When Comparing Objects to Migrate: The following symbols might appear *between* an object name and its check box to alert you to differences, as shown in Figure 3–17.

The Add icon, **+**, appears only when the object is present in one directory but *not* both:

- An + (Add icon) in the Source Environment list indicates that the object is present on the source directory but *not* on the target directory.
- An + (Add icon) in the Target Environment list indicates that the object is present on the target directory but *not* the source directory

The Diff icon (**!**) appears when the logical object has differing attribute values or dependents, or both.

Figure 3–17 shows an example with the following differences (among others):

- `Policy1` (displayed with the Add + icon) is present only in the source.
- `Policy2` (displayed with the Diff **!** icon) is the same logical object in the source and target but has different attribute values for the `Number of Login tries Allowed` and `Password Minimum Age` on the source and target.

  Steps to compare data are included in the procedure under "Migrating Data" on page 3-51.

Selecting Objects to Customize and Migrate: After comparing the differences between the source and target, you select the check box beside objects in the source tree that you want to migrate. When all desired objects are selected on the source, you click the Next button to display the Customize page. If you click Cancel, you are returned to the Select Logical Objects to Compare page.

The next step is to customize data on the target before migration, as described next.

About Customizing the Target

This topic introduces the method that you use to resolve differences in attribute values by applying optional transformation rules or by manually customizing attributes during migration. Step-by-step instructions are provided in "Migrating Data" on page 3-51.

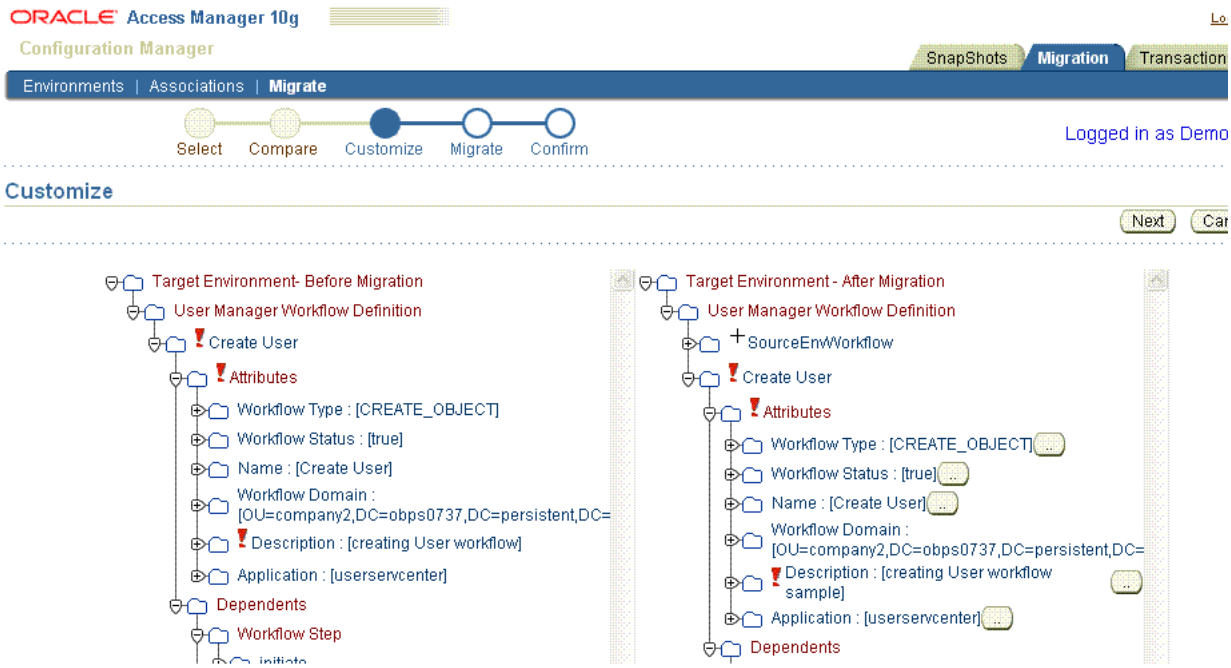
After you select logical objects on the Compare and Migrate page and click Next, any transformation rules that were defined for the association are applied automatically. The Customize page appears and shows how objects on the target have been customized by the application of the transformation rules, if any. In the progress indicator, Customize is highlighted.

Initially, only the titles of the two environments are shown. When you expand either environment, details of both environments are presented in a navigation tree:

- **Target Environment - Before Migration**: This pane shows the current and exact state of logical objects in the target LDAP directory *before* transformation rules and any manual customizations are applied.
- **Target Environment - After Migration**: This pane shows the state of logical objects on the target as they will be after transformation rules, manual customization, and migration are completed.

A sample Customize page is shown in Figure 3–18. In this example, objects are expanded. Differences in attributes and dependents are visible. Again, the Add (+) and the Diff (!) icons indicate differences between the target before and after migration.

Figure 3–18 Partial Customize Page

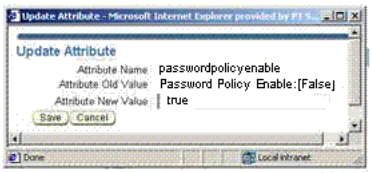


Clicking the Cancel button terminates the Customize operation and returns you to the Select Logical Object Types to Compare page.

Manually Customizing Attributes: Attributes in the Target Environment - After Migration tree include an update button labeled with two dots (..). Selecting an update button opens an Update Attribute window, where you can manually assign a new value for the attribute. The new value will be assigned during the data migration. Alternatively you can customize attributes after migration within your Oracle Access Manager 10*g* (10.1.4.0.1), or Oracle COREid Release 7.0.4, deployment.

For example suppose that in both views the `Password Policy Enable` attribute is `(False)`. To manually customize the value of this attribute, you select the (..) button beside `Password Policy Enable (False)`. In the Update Attribute window, you enter a new value, in this case `true`, and save it. Figure 3–19 provides an example of the Update Attribute window.

Figure 3–19 Update Attribute Window



When you click Save, you are returned to the Customize page and the new value is reflected in the Target Environment - After Migration tree. If you canceled the update, you are returned to the Customize page with no changes made to the attribute.

When you finish customizing attributes and click the Next button the Preview page appears, as described next.

About Previewing Before Migration

This topic introduces the method that you use to preview all data that will be migrated before the operation is performed. Step-by-step instructions are provided in "Migrating Data" on page 3-51.

The Preview page provides you with a final opportunity to evaluate any customizations and to verify the logical objects that will be migrated. In the progress indicator, Migrate is highlighted.

On the Preview page, you expand icons as you did on other pages. The Diff (!) icon appears *only* to identify attribute value differences on the target before and after the migration.

Before you click the Migrate button you must enter a unique transaction description to identity this specific migration operation, as described next.

Clicking the Back button returns you to the Customize page. Clicking the Cancel button returns you to the initial Select Logical Objects to Compare page, with nothing selected.

About Transactions and Migrating the Data

This discussion introduces you to the method you use to enter a unique transaction description before migrating the data. Step-by-step instructions are provided in "Migrating Data" on page 3-51.

A unique numeric Transaction ID is assigned automatically during data migration. Before you click the Migrate button, Oracle recommends that you enter a unique transaction description in the field provided at the *bottom* of the Preview page. A unique description will help identity this transaction from others later on. You can use a transaction record to roll back any changes made during this migration, as described in Chapter 5.

When you click the Migrate button, data migration begins. When migration completes, an informational message appears stating that the operation was successful. For details about the time to complete data migration, see "Downtime Assessment and Example" on page 1-15.

Note: Alternatively, you can choose to export data to an ldif file, as described next.

After migrating data, you must restart all Identity and Access Servers in the target deployment, as described in "Restarting Servers After Migration" on page 3-55.

About Exporting Data to an LDIF File (Optional)

This discussion introduces you to an alternative method to migrating data automatically. Step-by-step instructions are provided in "Migrating Data" on page 3-51.

Oracle Access Manager Configuration Manager enables you to export data to an LDIF file instead of migrating data automatically. If you export data to an LDIF file, you can edit the LDIF file offline using a text editor, if desired, then import the LDIF file using an external tool offline.

The export method includes using Oracle Access Manager Configuration Manager to select an association, select logical object types on the source, and compare selected objects on the source with those on the target. You can also preview changes after the

application of transformation rules and customize data manually using the Configuration Manager if you choose. However, instead of assigning a transaction description and migrating data with the Configuration Manager, you export your selections to an LDIF file.

After exporting data to an LDIF file, you import it offline at a later time. No transaction record is created in this case, because the actual migration occurs independently. Without a transaction record, rolling back changes is not possible using Oracle Access Manager Configuration Manager.

Steps to export data to an LDIF file are included in the procedure on "Migrating Data", next. In this case, Oracle recommends that you make a snapshot of the target directory just before importing the LDIF file using an external tool.

Note: Details of importing the LDIF file are outside the scope of this manual.

Whether you export data to an LDIF file or migrate data automatically using the Configuration Manager, you must restart all Identity and Access Servers in the target deployment. For more information, see "Restarting Servers After Migration" on page 3-55.

Migrating Data

This topic provides the prerequisite tasks and the procedure to migrate data.

Any individual with `HMUser` privileges can perform data migration. The repository for Oracle Access Manager Configuration Manager and the associated LDAP directories must be online. Confirm that all prerequisite tasks in Table 3–8 are completed before you use the procedure in this section to migrate data.

Table 3–8 Migration Prerequisites

Confirm	Prerequisite Tasks	Look in
	Notify administrators of the migration window in advance (and follow up after migration).	Notifying Other Administrators on page 3-3
	Create at least one directory association to specify the source and target for the migration.	Creating a Directory Association on page 3-15
	Add (optional) transformation rules for the association.	Adding an Optional Transformation Rule on page 3-34
	Make a snapshot of the current state of the target directory.	Creating a Snapshot on page 3-39

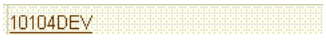
To migrate data from the source to the target

1. **Test Environment**: Perform the following activities to confirm that the source and target environments in the association are accessible to the Configuration Manager:

   a. From Oracle Access Manager Configuration Manager, click the Migration tab, click Environments. For example:

      Migration, Environments

   b. Click the source environment name to view details. For example:



c. On the View Environment page, click the Test Environment button.

Test Environment

d. Read the informational message to confirm that the environment connection is successful.

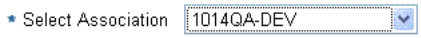
If there is any problem with the connection, notify the directory administrator. The directory must be live and online during the migration.

e. Repeat these activities with the target environment to ensure that it is live and online.

2. From Oracle Access Manager Configuration Manager, click the Migration tab, then click Migrate:

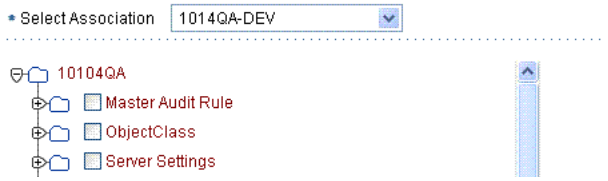
Migration, Migrate

3. From the Select Association list, choose the desired association. For example:



4. Perform the following steps to select logical objects to compare and migrate:

a. Expand the association icon to display a list of supported logical object types. For example:



b. Select all of the logical object types that you want to include in this migration.

5. **Compare**: Perform the following steps to compare differences and view dependents of selected logical object types on the source and target directories:

a. Click the Compare button to display the Compare and Migrate page. For example:

Compare

The Compare and Migrate page appears.

b. **Show Differences:** On the Compare and Migrate page, perform the following steps to review any differences:

– Expand objects by clicking the expansion icon beside the folder.

– Add + icon: Determine whether the Add icon is only in the target, or only in the source. For more information, see "About Comparing Data Before Migration" on page 3-46.

– Diff ! icon: Determine which objects are designated with the Diff (!) icon. This indicates differences for attribute values or dependents. For more information, see "About Comparing Data Before Migration" on page 3-46.

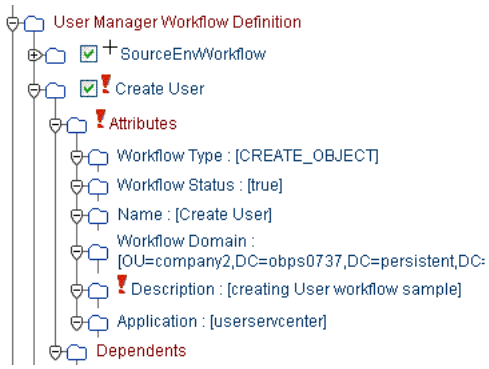
c. **Show Dependents**: Perform the following activities to show dependents for a logical object:

   – Click the expansion icon beside a logical object to expand it.

   – Look for and expand the list of dependents and attributes.

   Dependents are migrated automatically; there is no way to select these independently. However, you must select logical objects and related logical objects to migrate.

d. **Select Logical Objects and Related Objects for Migration**: From the Source, check the box beside each item that you want to select (or click a checked box to clear it).



e. On the Compare and Migrate page, click the Next button to display the Customize page.

   Next

   For more information about comparing logical objects, see "About Comparing Data Before Migration" on page 3-46.

When you click the Next button, any transformation rules created for this association are applied automatically. The Customize page appears. The body of the page is divided in two segments: Target Environment - Before Migration and Target Environment - After Migration.

6. **Customize**: On the Customize page, perform the following activities:

   a. Review details of the Target Environment - After Migration to see how the application of any transformation rules has changed objects.

   b. Observe and document differences between the Target Environment - After Migration and the Target Environment - Before Migration; pay attention to any item flagged with the Diff (!) icon because you might want to update attributes.

   c. Proceed as desired for your environment:

      – **Update Attributes Before Migration**: Proceed to step 7 if you want to perform this optional activity.

      – **Preview Data**: Proceed to Step 8 to review all information before migration.

      – **Cancel the Migration:** Click the Cancel button to return to the Select Logical Objects to Compare page.

      For more information, see "About Customizing the Target" on page 3-48.

7. **Update Attributes**: From the Customize page, perform the following optional activities if desired. After expanding objects in the Target Environment - After Migration list:
   a. In your browser window, enable pop-up windows for this site.
   b. Click the update button (..) beside the attribute that you want to change to open the Update Attributes window. For example:

   c. In the Update Attributes window, add the new value and click Save. For example:
      – **Attribute Name**: The current attribute name is fixed and cannot be changed.
      – **Attribute Old Value**: The current attribute value is fixed.
      – **Attribute New Value**: Enter the new attribute value that you want to assign using guidelines in "About Customizing the Target" on page 3-48.
      – **Save**: Click the Save button to save the updated attribute value and return to the Customization page.
      – Repeat as needed for each attribute that you want to change in the Target Environment - After Migration list.
   d. When you finish with the Customize page, click the Next button to call the Preview page.
8. **Preview the Target**: On the Preview page, expand icons and review all information to confirm that this is what you want to migrate, then proceed as appropriate for your migration. For example:
   – **Export Data to an LDIF File:** Proceed to Step 9 to export data to an LDIF file for customizing or importing with an external tool. In this case, no transaction record is created.
   – **Migrate Data Now:** Skip to Step 10 to assign a transaction description then continue with following steps.
   – **Cancel the Migration:** Click the Cancel button to return to the Select Logical Objects to Compare page.
9. **Export to LDIF File (Optional)**: Use the following steps only to *export* the selected logical objects to an LDIF file (to import offline at a later time).
   a. Click the Export to LDIF button.

      Export to LDIF

   b. In the Open MigrationData window, click Open with Notepad (default).

      Open with Notepad (default)

   c. In the Notepad window, you can review and edit the data to be exported, then click Save.

      Save

   d. In the Save as window locate the destination directory for this file, enter a file name with the .ldif extension, then click Save. For example:

```
MigrationData_12_16.ldif
```

The file is created in the location you specify. No transaction record is created. For more information, see "About Exporting Data to an LDIF File (Optional)" on page 3-50.

e. Before using an external tool to import the LDIF file, make a snapshot of the target directory. For more information, see "Creating a Snapshot" on page 3-39.

The use of external tools to migrate data using an LDIF file are outside the scope of this manual.

10. **Assign a Transaction Description (Required)**: In the Transaction Description field at the bottom of the Preview page:

    a. Enter a unique name to help you recognize the record of this specific transaction later on. For example:

    ```
    10104DevQA_12_14
    ```

    b. Click Save.

    Save

11. **Migrate Data**: On the Preview page, click the Migrate button. For example:

    Migrate

    A unique Transaction ID is assigned, and then the migration operation completes. The amount of time it takes to perform the migration depends on several factors. For more information, see "Downtime Assessment and Example" on page 1-15. An informational message confirms that the migration completed successfully as shown here. The transaction ID and description are also shown.

    Note: The informational message reminds you to restart all Identity Servers and Access Servers after successful migration. When migrating workflows for the User Manager, Group Manager, or Organization Manager, the message reminds you bo migrate the PPP plug-ins and PPP catalog files manually. When migrating authentication schemes, the message reminds you the migrate custom authentication plug-ins manually. When migration authorization schemes, the message reminds you to migrate customized authoirzation plugs-ins manuall.

12. Review the informational message to confirm success, then note the transaction ID assigned during the migration (and the description that you provided).

    After migration, you must shut down and restart all Identity Servers and Access Servers to flush the caches and update the configuration with the new information.

13. Proceed to "Restarting Servers After Migration" to ensure data synchronization after migration.

Restarting Servers After Migration

When you alter data directly using the Identity System Console or Access System Console, changes are automatically written to the directory from the server. In this

case, appropriate entries in the server cache are flushed and the server is updated with the latest configuration data automatically.

When you use Oracle Access Manager Configuration Manager to migrate changes, or you export data to an LDIF file and import it offline, changes are written to the directory only. In this case, the servers are not directly involved. As a result, immediately after migrating data with the Configuration Manager, you must manually restart all Identity Servers and Access Servers in the target environment to flush their caches and update the servers with the latest configuration data from the target directory.

Caution: When multiple servers are involved, it is particularly important to avoid delays that could result in data synchronization issues between the server and the directory. During a rolling restart, there will be a period of inconsistency until all servers have been restarted.

Restarting 10*g* (10.1.4.0.1) Policy Manager components (known in release 7.0.4 as the Access Manager component), is not required after data migration.

Caution: If you have a replicated directory environment, you must ensure that the migration changes made to the master LDAP directory are fully propagated to the replicas before restarting Identity and Access Servers.

To ensure data synchronization after migration

1. **Replicated Environment**: Immediately after migrating data, ensure that all changes have fully propagated to the replicas before performing the following steps.
2. Immediately after migrating data, restart all Identity Servers (Identity Server Service on Windows platforms) in the target installation.
3. Immediately after migrating data, restart all Access Servers (Access Server Service on Windows platforms) in the target installation.
4. Validate the target environment and data changes, as described in Chapter 4, "Validating Migration Success".

4

Validating Migration Success

This chapter suggests how to validate the success of a data migration performed using Oracle Access Manager Configuration Manager. This chapter includes the following sections:

About Validating Migrated Changes

As discussed in Chapter 1, Oracle recommends that you develop specific tests to help you quickly evaluate the configuration data changes in the source deployment before you began migrating data. After migration, you can use these same tests in the target deployment to ensure that everything is working as expected.

> **Caution:** Oracle strongly recommends that you reconcile any dependencies in the target deployment. For example if you migrated workflow data, ensure that all workflow participants mentioned in the source directory are included in the target. Otherwise, the workflow in the target deployment might not work properly.

Confirm that the prerequisite tasks outlined in Table 4–1 have been performed before you start the tasks in this chapter.

Table 4–1 Validation Prerequisites

Confirm	Prerequisite Tasks	Look in
	Develop tests in the source deployment that validate the success of configuration data changes to be migrated	Data Migration Planning and Deliverables on page 1-12
	Migrate data	Migrating Data on page 3-51
	Restart all Identity and Access Servers in the target deployment	Restarting Servers After Migration on page 3-55
	Ensure that all dependencies in the source are also in the target environment	"Physical Entries and Logical Objects" on page 1-7

For more information that you can use to ensure that the migrated data operates properly, see the following topics:

- Validating Migrated Data with Oracle Access Manager 10g (10.1.4.0.1)

- Validating Migrated Data with Oracle COREid Release 7.0.4

Note: The procedures that you perform to validate the success of the migration in a live target deployment are essentially the same regardless of your product release (10*g* (10.1.4.0.1) or release 7.0.4). Only certain product terms differ.

Validating Migrated Data with Oracle Access Manager 10*g* (10.1.4.0.1)

Oracle recommends that you use the migrated data in your Oracle Access Manager 10*g* (10.1.4.0.1) deployment to ensure that the changes were properly migrated and everything is working as expected.

Refer to the following topics for details about validating migrated data within your target Oracle Access Manager 10*g* (10.1.4.0.1) deployment:

- Validating Identity System Data Migration in 10g (10.1.4.0.1)
- Validating Access System Data Migration in 10g (10.1.4.0.1)

Validating Identity System Data Migration in 10*g* (10.1.4.0.1)

To validate data migration in the Identity System, you will perform tasks in the Oracle Access Manager 10*g* (10.1.4.0.1) Identity System Console and applications that rely on the target directory and migrated data.

The following procedure provides steps and an outline of activities that you might perform to validate migrated data. Step 5 includes several suggestions about activities that you might want to perform. However, the actual tasks that you perform will depend on the data that you have migrated.

To validate 10*g* (10.1.4.0.1) Identity System data migration

1. Identify the Identity System applications and functions that are affected by the migrated data and develop a plan to test these in the target Identity System and applications.
2. In the target deployment, ensure that all Identity Server services and WebPass Web server instances are running.
3. Go to the Identity System Console from your browser by specifying the appropriate URL for your deployment. For example:

   ```
   http://hostname:port/identity/oblix
   ```

   In the sample URL, *hostname* refers to computer that hosts the Web server; *port* refers to the HTTP port number of the WebPass Web server instance; /identity/oblix connects to the Identity System Console.

   The Oracle Access Manager landing page appears. If it does not appear, ensure that the WebPass Web server is active.
4. Perform any of the following tasks, or others, to prove that the migrated data is operating properly:
   - Review panels in the User Manager, Group Manager, or Organization Manager.
   - Verify audit policies for the User Manager, Group Manager, or Organization Manager, if these are affected.

- Review attribute access control policies in the User Manager, Group Manager, or Organization Manager
- Review the Master Auditing Policy and the Global Auditing Policy, if appropriate.
- Verify Password and Lost Password policies, if such data changes were migrated.
- Validate any migrated workflow configuration details, when such data changes were migrated.
- Review object class definitions, if appropriate after migration.
- Verify Identity Server and WebPass definitions; server settings; administrator information; and directory options.

5. Log out, as usual.

For information about performing specific tasks, see the *Oracle Access Manager Identity and Common Administration Guide*.

Validating Access System Data Migration in 10*g* (10.1.4.0.1)

To validate data migration in the Access System, you will perform tasks in the Oracle Access Manager 10*g* (10.1.4.0.1) Access System Console and applications that rely on the target directory and migrated data.

The following procedure provides steps and an outline of activities that you might perform to validate migrated data. Step 5 includes several suggestions about activities that you might want to perform. However, the actual tasks that you perform will depend on the data that you have migrated.

To verify a successful 10*g* (10.1.4.0.1) Access System data migration

1. Identify the Access System applications and functions that are affected by your migrated data and develop a plan to test these.
2. Ensure all Policy Manager Web server and WebPass Web server instances are running.
3. Go to the Access System Console from your browser by specifying the appropriate URL for your deployment. For example:

   ```
   http://hostname:port/access/oblix
   ```

   In the sample URL, *hostname* refers to computer that hosts the Web server; *port* refers to the HTTP port number of the WebPass Web server instance; /access/oblix connects to the Access System Console.

   The Oracle Access Manager landing page appears.
4. **Landing Page Does Not Appear**: Ensure that the WebPass Web server is live and online.
5. Log in as a Master Administrator.
6. Perform one or more of the following tasks, or others, to validate migrated data:
   - Review Access Server, Access Server Cluster, and Access Client details.
   - Validate authentication and authorization scheme details that are affected.
   - Examine reports data.
   - Review affected policy domains.

7. Log out, as usual.

For more information about performing specific tasks, see *Oracle Access Manager Access Administration Guide*.

Validating Migrated Data with Oracle COREid Release 7.0.4

Oracle recommends that you use the migrated data in your Oracle COREid Release 7.0.4 deployment to ensure that the changes were properly migrated and everything is working as expected.

The following procedures describe how to validate successful data migrations in Oracle COREid Release 7.0.4:

- Validating Identity System Data Migration in Oracle COREid Release 7.0.4
- Validating Access System Data Migration in Oracle COREid Release 7.0.4

> **Note:** The procedures that you complete to validate the success of the migration in a live target deployment are essentially the same regardless of your product release (10*g* (10.1.4.0.1) versus release 7.0.4). Only certain product terms differ.

Validating Identity System Data Migration in Oracle COREid Release 7.0.4

To validate data migration in the Identity System, you will perform tasks in the Oracle COREid Release 7.0.4 System Console and applications that rely on the target directory and migrated data.

The following procedure provides steps and an outline of activities that you might perform to validate migrated data. Step 5 includes several suggestions about activities that you might want to perform. However, the actual tasks that you perform will depend on the data that you have migrated.

To validate Identity System data migration in release 7.0.4

1. Identify the Identity System applications and functions that are affected by your migrated data and develop a plan to test these.
2. Ensure all Identity Server services and WebPass Web server instances are running.
3. Go to the COREid System Console from your browser by specifying the appropriate URL for your deployment. For example:

   ```
   http://hostname:port/identity/oblix
   ```

   In the sample URL, *hostname* refers to computer that hosts the Web server; *port* refers to the HTTP port number of the WebPass Web server instance; /identity/oblix connects to the COREid System Console.

   The COREid landing page appears.
4. **Landing Page Does Not Appear**: Ensure that the WebPass Web server is live and online.
5. Log in as a Master Administrator.
6. Using the COREid System Console or applications, perform the following tasks, or others, to validate data that can be affected by the migration:

- Review panels in the User Manager, Group Manager, or Organization Manager.
- Verify audit policies for the User Manager, Group Manager, or Organization Manager, if these are affected.
- Review attribute access control policies in the User Manager, Group Manager, or Organization Manager
- Review the Master Auditing Policy and the Global Auditing Policy, if appropriate.
- Verify Password and Lost Password policies, if such data changes were migrated.
- Validate any migrated workflow configuration details, when such data changes were migrated.
- Review object class definitions, if appropriate, after migration.
- Verify Identity Server and WebPass definitions; server settings; administrator information; and directory options.

7. Log out, as usual.

For more information about performing specific tasks, see the *Oracle COREid Access and Identity Administration Guide Volume 1*.

Validating Access System Data Migration in Oracle COREid Release 7.0.4

To validate data migration in the Access System, you will perform tasks in the Oracle COREid Release 7.0.4 Access System Console and applications that rely on the target directory and migrated data.

The following procedure provides steps and an outline of activities that you might perform to validate migrated data. Step 5 includes several suggestions about activities that you might want to perform. However, the actual tasks that you perform will depend on the data that you have migrated.

To verify a successful Access System data migration in release 7.0.4

1. Identify the Access System applications and functions that are affected by your migrated data and develop a plan to test these.
2. Ensure your Access Manager Web server and WebPass Web server instances are running.
3. Go to the Access System Console from your browser by specifying the appropriate URL for your deployment. For example:

   ```
   http://hostname:port/access/oblix
   ```

   In the sample URL, *hostname* refers to computer that hosts the Web server; port refers to the HTTP port number of the WebPass Web server instance; /access/oblix connects to the Access System Console.

   The Access System landing page appears.

4. **Landing Page Does Not Appear**: Ensure that the WebPass Web server is live and online.
5. Log in to the Access Manager/Access System Console as a Master Administrator.
6. Perform any of the following tasks, or others, to validate the migrated data:

- Review Access Server, Access Server Cluster, and Access Client details.
- Validate authentication and authorization scheme details that are affected.
- Examine reports data.
- Review affected policy domains.

7. Log out, as usual.

For more information about specific tasks, see *Oracle COREid Access and Identity Administration Guide Volume 2*.

5

Managing Transactions and Rolling Back Changes

This chapter explains how to view transaction records created by Oracle Access Manager Configuration Manager during migration and how to roll back changes for a specific transaction. This chapter also discusses how to restore the content of a specific environment snapshot made using the Configuration Manager. This chapter includes the following sections:

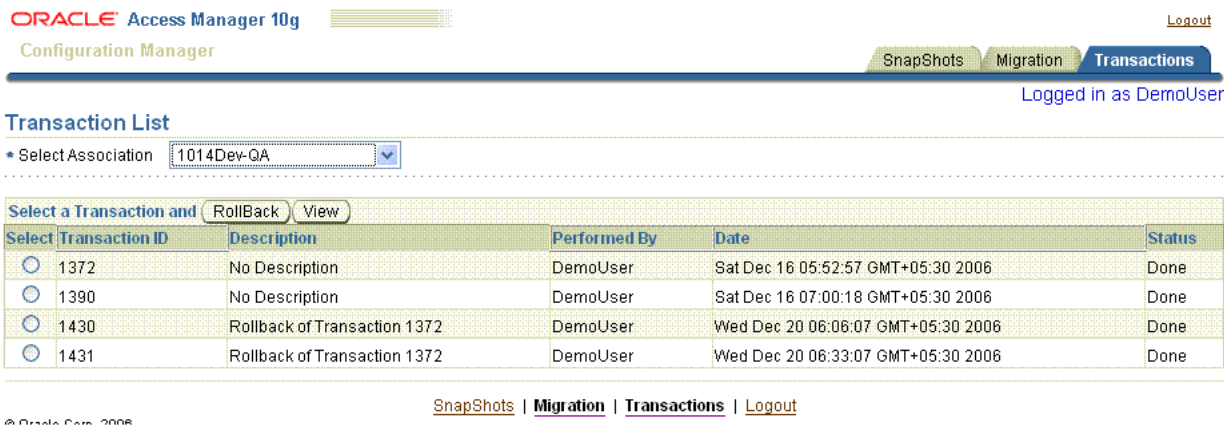
- Viewing Transaction Details for an Associated Directory Pair
- Rolling Back Changes Made During a Specific Transaction
- Exporting Transaction Data to an LDIF
- Restoring the Content of a Snapshot

Viewing Transaction Details for an Associated Directory Pair

A transaction record is created automatically each time that you perform a migration with Oracle Access Manager Configuration Manager. From the Transaction List page, you can select an association and view existing transaction records for that association.

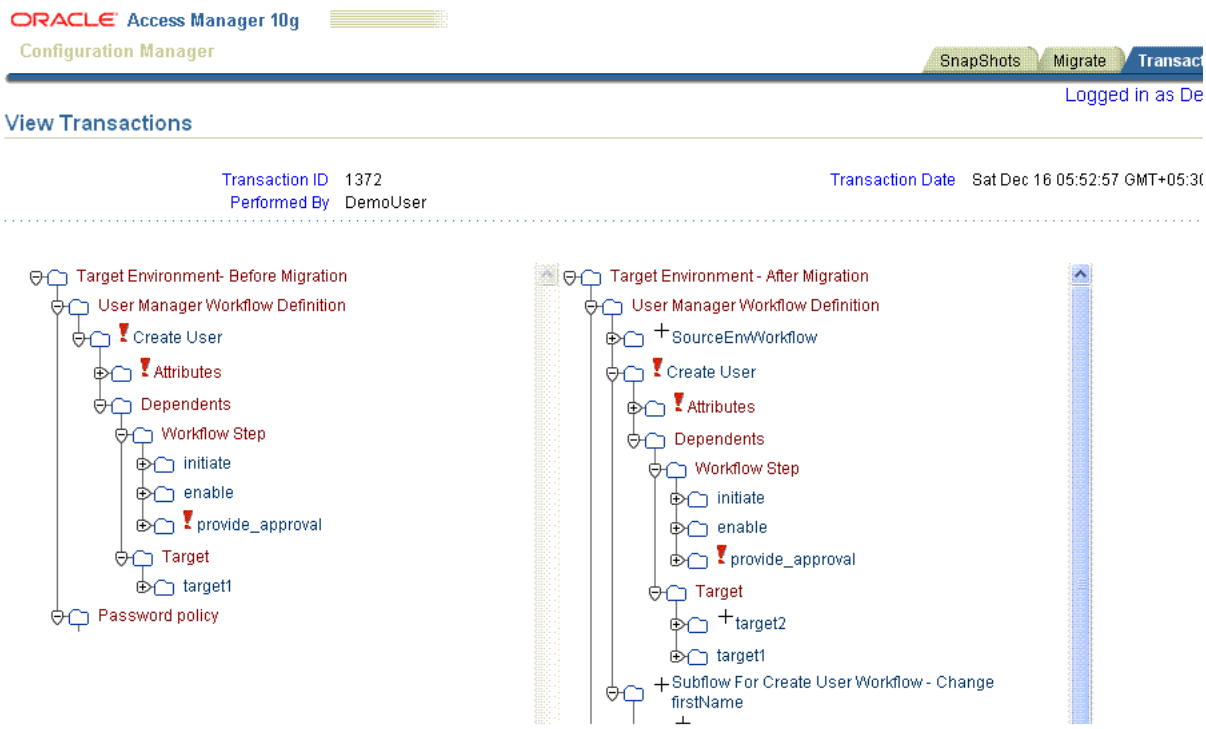
Figure 5–1 shows a sample Transaction List page. Details you can view include the Transaction ID assigned automatically during the migration, the description that was entered for the transaction, the name of the user who performed the migration the date on which the migration was performed, and the status of the migration transaction.

Figure 5–1 Transaction List Page



You can select a transaction record to view the changes made during the selected migration in greater detail. Figure 5–2 shows an example of the View Transactions page and the types of details that you can view for the selected migration transaction.

Figure 5–2 Viewing Differences Between the Target Before and After Migration



As shown in Figure 5–2, each folder has an expansion icon. Symbols appear between the folder icon and the object name to indicate that the following types of changes occurred during the migration:

- **+**: Add Icon (+) appears when the object is present in one directory but *not* both.
- **!**: The Diff Icon (!) appears when the logical object has differing attribute values or dependents.

If you have used Oracle Access Manager Configuration Manager to migrate data, you have seen these symbols when comparing and customizing the target. For more information about the symbols used to show differences, see "About Customizing the Target" on page 3-48.

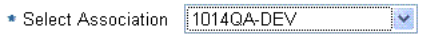
Note: You cannot explicitly delete a transaction record. Transaction records are deleted only when you delete the association to which the records belong.

To view transaction details

1. From Oracle Access Manager Configuration Manager, click the Transactions tab. For example:

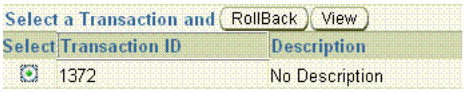
   Transactions

2. From the Select Association list, select the desired directory association. For example:



   The Transactions List page appears, with existing transactions for the selected association.

3. In the Select column, click the option beside the desired transaction ID to select it. For example:



4. Click the View button to display the details of this transaction. For example:

   View

5. Review the details in the transaction record to ensure that this is what you want.

6. Click the Back button on this page to return to the Transaction List page. For example:

   Back

Rolling Back Changes Made During a Specific Transaction

You can select a transaction record, then undo (**roll back**) the changes made during data migration using Oracle Access Manager Configuration Manager. Rolling back a transaction undoes only those changes made to logical objects during data migration using Oracle Access Manager Configuration Manager.

There are any number of reasons you can choose to roll back a migration transaction. For example, consider a scenario where you changed logical objects in the source deployment (workflows, policy domains, and WebGates). After testing and validating that the changes produced the desired result in the source deployment, you migrated the data to a target deployment. However, if postmigration testing in the target deployment did not produce the results you expected, you can choose to roll back the transaction to restore the target environment. Considering a different scenario, suppose that you migrate and validate a change to one object in the target environment, and then decide to delete the object from the target. In this case, you can either roll back the transaction to remove the migrated logical object from the target or delete it directly using the Identity or Access System Console.

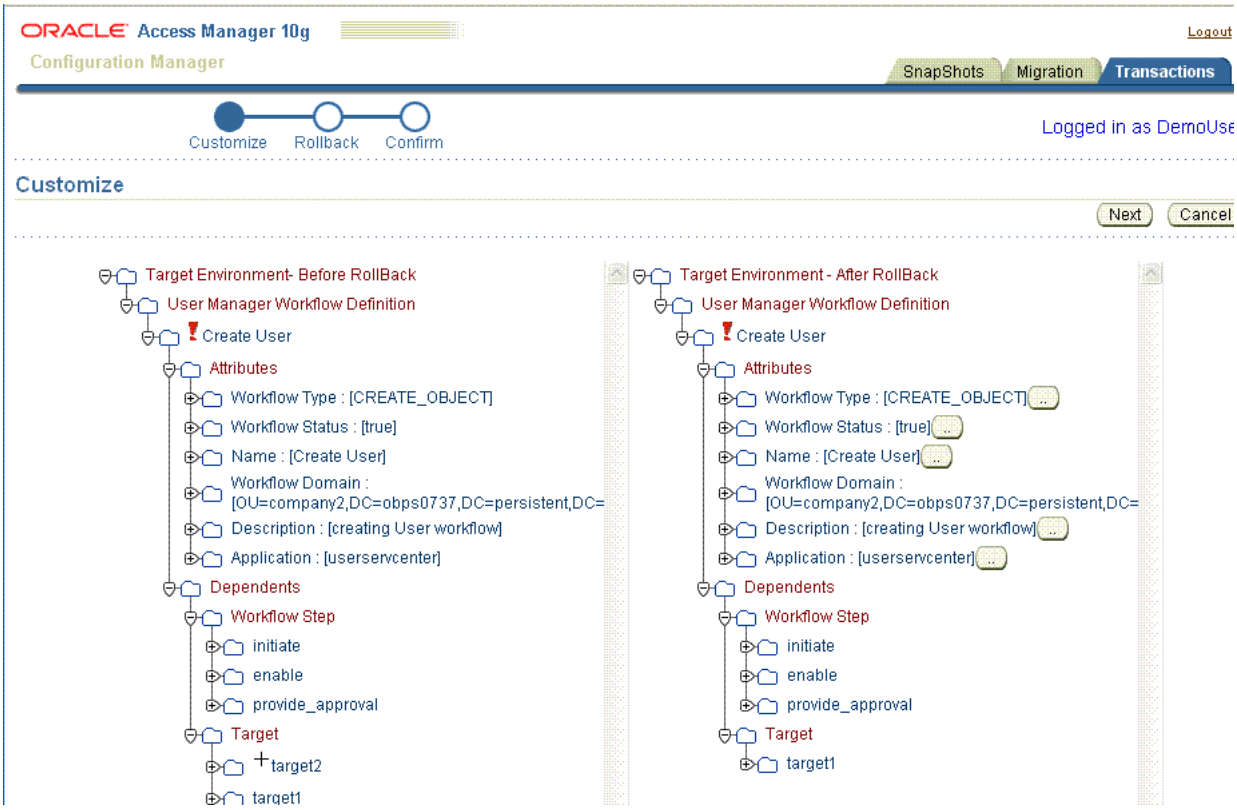
Before you perform a rollback, be sure to confirm that the environment involved is accessible by the Configuration Manager. When you roll back a transaction, Oracle Access Manager Configuration Manager returns the target environment to the state it was in before the migration by:

- Removing logical objects on the target that were added during the migration.
- Restoring logical objects on the target to their state before migration, which means that:
  - Migrated logic objects that had different attributes or dependents before migration are reverted to their premigration state.

- Transformation rules that were applied are undone during the rollback operation. Logical objects that were affected by the application of transformation rules are restored to their premigration state.
- Any manual customizations made to attribute values during the migration are undone during the rollback operation.

Following is a brief overview of the rollback process. After you select the environment and initiate the rollback operation a Customize page appears, as shown in Figure 5–3. Scroll bars are provided, as usual. In the progress indicator, Customize is highlighted.

Figure 5–3 Customize Page During the Rollback Operation



The rollback Customize page provides a navigation tree of the:

- **Target Environment - Before Rollback**: The target as it is now, *after* the migration transaction and *before* this rollback operation.
- **Target Environment - After Rollback**: The target as it *will be* after this rollback operation. The rollback operation returns the target to this premigration state. It is in this view that you can customize attributes before rolling back the changes.

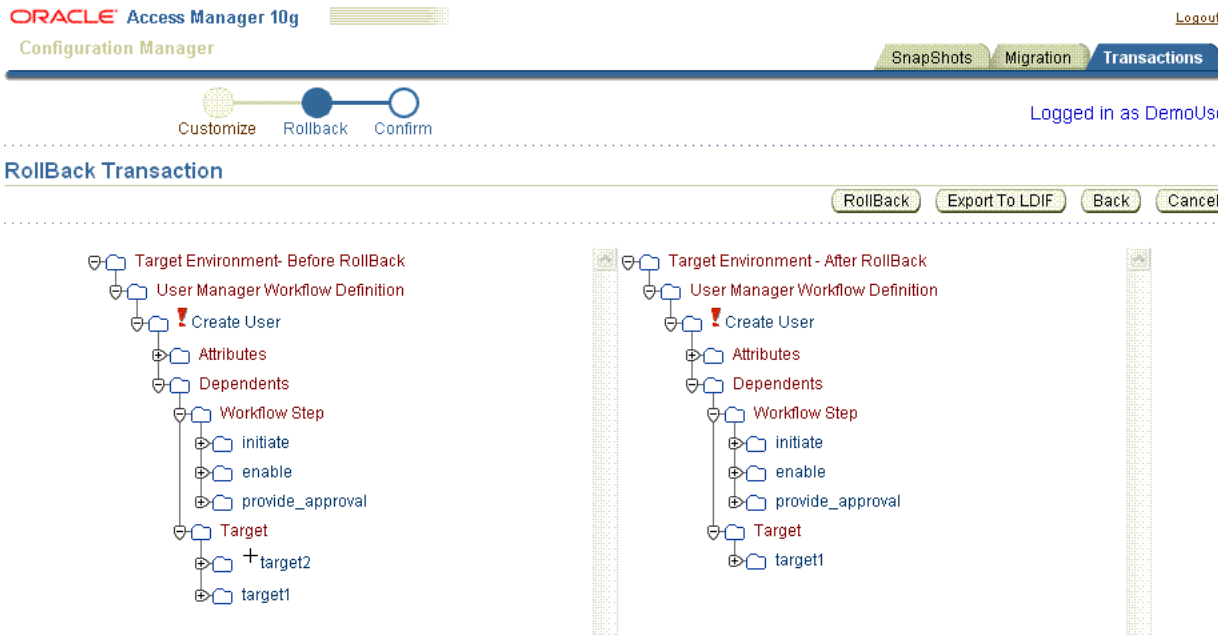
On the Customize page, symbols that appear between the folder icon and the object name indicates the following types of changes:

- The Add oIcon (+) appears only when the object is present in one directory but not both.
- **!**The Diff Icon (!!) appears when the logical object has differing attribute values or dependents.

From the Customize page, you can manually update attributes in the Target Environment - After Rollback view. The process is similar to the customization that you can perform during migration. For more information about customizing attributes, see "About Customizing the Target" on page 3-48.

Whether you customize attributes or not, you click the Next button to proceed to the Rollback Transaction page. A sample Rollback Transaction page is shown in Figure 5–4.

Figure 5–4 Rollback Transaction Page



The Rollback Transaction page enables a final review and validation before the actual rollback. The page shows the target both as it is now (before) and as it will be (after) this rollback operation. In the progress indicator, Rollback is highlighted.

The Rollback Transaction page includes four buttons, and a Transaction Description field where you enter a unique description for the record that will be created during this rollback operation. You can use the new transaction to roll back this rollback operation and restore the target to the state it is in at this moment (after the original migration and before rolling back changes).

The Rollback Transaction page includes the following buttons:

- **Rollback:** Use the Rollback button to undo the changes made during the selected transaction and restore the environment to the condition you see in the Target Environment - After Rollback view, as described in the following procedure.

  You are asked to verify that this is what you want to do. When the operation completes, you are notified with an informational message that appears on the Confirm page. A transaction record is created for this rollback operation.

- **Export to LDIF File**: Use the Export to LDIF File button to create an optional LDIF file that contains data in the Target Environment - After Rollback view. You can use this LDIF file to edit or import the data using an external tool. In this case, no transaction record is created.

- **Back**: Use the Back button to return to the Customize page where you can update attributes.
- **Cancel**: Use the Cancel button to terminate the rollback operation without completing it and return to the Transaction List page.

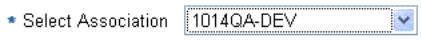
The following procedure provides the steps that you use to perform the rollback operation. Details about exporting data to an LDIF file and customizing attributes are included in the procedure and are optional.

To roll back the changes made during a specific migration transaction

1. In the Configuration Manager, select the Transactions tab. For example:

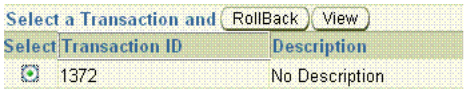
   Transactions

2. From the Select Association list, select the desired directory association. For example:

   The Transactions List page appears with existing transactions for the selected association.

3. Click the option beside the desired transaction to select it.

4. Click the Rollback button:

   Rollback

5. **Customize Attributes (Optional)**: Perform the following optional steps to update attributes manually; new values are assigned during the rollback operation. Otherwise, click Next and skip to Step 6.

   a. On the Customize page, click the button labeled (..) beside the attribute that you want to change (to open the Update Attributes window).

   b. In the Update Attribute window, add the new value and click Save. For example:

      – **Attribute Name**: The current attribute name is fixed and cannot be changed.

      – **Attribute Old Value**: The current attribute value.

      – **Attribute New Value**: Enter the new attribute value in the field provided.

      – **Save**: Click the Save button to save the updated attribute value and return to the Customization page.

   c. Repeat Steps a and b for each attribute that you want to change in the After Rollback view.

   d. When you finish with the Customize page, click the Next button to display the Rollback Transaction page, then proceed with one of the following activities:

- **Export Data to an LDIF File:** Proceed to Step 6 if you want to create an optional LDIF file to edit or use when importing data with an external tool. No transaction record is created.
- **Roll Back Changes:** Proceed to Step 7 to create a transaction record and roll back changes.
- **Cancel the Rollback Operation:** Click Cancel to terminate the Rollback operation without completing it.

6. **Export to LDIF File (Optional)**: Perform the following steps, in order, only if you want to export the data to an LDIF file to import using an external tool. Otherwise, skip to step 7.
   a. On the Rollback Transaction page, click the Export to LDIF button:

      Export to LDIF

   b. In the Open MigrationData window, select a text editor (or click Open with Notepad (default)). For example:

      Open with Notepad (default)

   c. In the Notepad window review and edit the data to be exported, then save the file. For example:

      Save

   d. In the Save as window locate the destination directory for this file, enter a file name with the .ldif extension, and then click Save. For example.

      ```
      MigrationData_01_07.ldif
      ```

      The file is created in the location that you specify. No transaction record is created.

   e. Before using an external tool to import the LDIF file, make a snapshot of the target directory, as described in "Creating a Snapshot" on page 3-39.

7. **Roll Back**: On the Rollback Transaction page, complete the following activities to complete the operation:
   a. Enter a Transaction Description in the field provided, to name the record that is created during this rollback operation. For example:

      ```
      Roll back of Transaction 1372
      ```

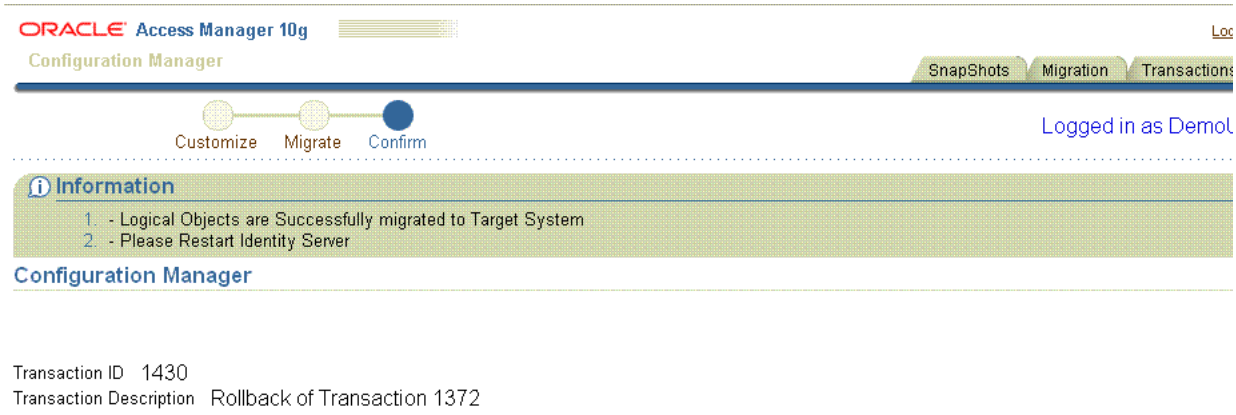
   b. Click the Rollback button to undo the changes that were made during the original migration transaction. For example:

      Rollback

   c. Click OK to validate and start the rollback operation. For example:

      OK

   d. Check the informational message when the operation completes, to confirm that the rollback is successful, as shown next.



8. Restart Identity and Access Servers to ensure data synchronization after migration, as described in "Restarting Servers After Migration" on page 3-55.

Exporting Transaction Data to an LDIF

Rather than using the automated Configuration Manager process to roll back changes made during a specific migration transaction, you can choose to export the details of a transaction record to an LDIF.

This operation is similar to the one described in "Rolling Back Changes Made During a Specific Transaction". However, in this case you will not complete the rollback operation using the Configuration Manager. Instead, you export the transaction record to an LDIF. Later you can edit the attributes in the record using a text editor, then use an external program to import the data. Importing data using an LDIF is outside the scope of this book.

During the export operation you are asked to provide a name for the transaction data LDIF. The default name is `MigrationData`. Oracle recommends that you rename this file and perhaps include the transaction ID assigned during the migration to help you identify it later (especially if you have more than one transaction LDIF).

To export the changes made during a specific migration to an LDIF

1. From the Configuration Manager home page, select the Transactions tab then select the desired directory association. For example:

   Transactions

   Desired Association

2. From the Transaction List, select the transaction and click the Export to LDIF button. For example:

   Desired Transaction

   Export to LDIF

3. In the Security Warning window, click Save. For example:

   Save

4. In the Save as window, locate the destination directory for this file and enter a file name with the .ldif extension then click Save. For example:

   TransactionIDData.ldif

   The file is created in the location you specify.

Restoring the Content of a Snapshot

This information is repeated from Chapter 3 for your convenience.

You might want to restore a snapshot if configuration data in the `oblix` tree of the environment becomes inconsistent or is corrupted as a result of changes that are external to Oracle Access Manager Configuration Manager. Any individual with `HMUser` privileges can perform this task. The repository for Oracle Access Manager Configuration Manager and the appropriate LDAP directory environment must be online.

When you restore a snapshot that was made using Oracle Access Manager Configuration Manager, the entire `oblix` tree is restored to the directory. Changes that are undone when you restore the snapshot include both migration changes that were made using the Configuration Manager, as well as changes that were made outside the Configuration Manager after data migration.

Caution: Restoring a snapshot will undo all changes made after the snapshot was taken and returns the directory to the state it was in at the time the snapshot was made.

Before the restoration commences, you are asked to verify that you want to restore the selected snapshot. After your verification, a new snapshot is created to capture the current state of the directory, and then the selected earlier snapshot is restored. If you believe that too many changes were undone during the restoration, you can restore the snapshot that was made during the restoration.

Note: If you created a directory backup using any application other than Oracle Access Manager Configuration Manager, you cannot use the Configuration Manager to restore the backup.

To restore the content of a snapshot

1. From Oracle Access Manager Configuration Manager, click the SnapShots tab. For example:

   SnapShots

2. Select an environment from the Select Environment list. For example:

3. In the Select column, click the option beside the name of the snapshot that you want to restore. For example:

4. Click the Restore button. For example:

   Restore

   A message asks you to verify that you want to complete the Restore operation, which returns the `oblix` tree in the environment to its previous condition.

5. Click OK to complete the restoration (or Cancel to terminate the operation).

OK

After you verify the operation, a new snapshot is made of the environment in its current state, and then the content of the selected snapshot is restored.

6. On the SnapShots List, review the informational message to confirm success; you should see the new snapshot details in the table.

A

Planning Worksheets and Tracking Checklists

Before migrating data, your team must create a document that defines and records a detailed plan for each installed deployment. You also need details about components and data within each deployment. This chapter provides the worksheet templates that you can copy and fill in, and checklists that you can copy and use to track migration activities:

About Completing Planning Worksheets and Checklists

Oracle recommends that you copy and fill in the worksheets in this appendix to record the details for each installed deployment. Oracle Access Manager installation and upgrade worksheets provide a starting point. Any details that you can access and print from your deployment will save you time and eliminate the possibility of errors.

> **Note:** Store worksheets, printed copies, and other recorded details about your installation in a secure location for tracking purposes.

This appendix also provides three checklists. You use the first checklist to track application deployment and setup. You use the second checklist to track data

migration activities. The third checklist identifies data that is not supported for migration using Oracle Access Manager Configuration Manager.

Worksheet for Your Overall Deployment

Use the space in Table A–1 to record general information about your deployment.

Table A–1 Details for Your Overall Deployment

Task	Subtask	Overall Deployment Worksheet
0	0.1	**Deployment Name**: _____ **Deployment Type** (*circle all that apply*): _____Identity System Only or _____Joint Identity and Access System _____Development_____Test/Demo_____QA_____Preproduction_____Production _____Other Master Administrator for this deployment:_____ Date of the last validation of system operation:_____
	0.2	**Total number of each component in this deployment**: Identity Servers:_____ WebPass Instances:_____ **If This is a Joint Identity and Access System, enter the total number of**: Policy Managers (release 7.0.4 known as Access Manager component):_____ Access Servers:_____ WebGates:_____ Custom AccessGates:_____ Application Server Connectors (BEA, IBM, OC4J):_____
	0.3	**Total number of**: Directory Instances for Identity Servers only:_____ **If This is a Joint Identity and Access System**: Directory Instances for Policy Managers only:_____ Directory Instances used by Identity Servers, Policy Managers (release 7.0.4 Access Manager), Access Server:_____
	0.4	**Applications that depend on this deployment, owner**: App. Names _____ Owner _____ Comments_____ _____ _____ _____ _____ _____
	0.5	Change control procedures:_____ _____ Scheduled maintenance windows:_____ _____ Off-peak hours operation windows:_____ _____

Worksheet for Directory Instances

Use the space in Table A–2 to record details about each directory instance in Oracle Access Manager 10*g* (10.1.4.0.1), or Oracle COREid Release 7.0.4, deployments.

Table A–2 Details for Directory Instances

Task	Subtask	Directory Instance Details
1	1.1	Directory server type: _____ Directory server version:_____ Directory server patch level:_____
	1.2	Directory Server Details Directory server DNS host name/IP address:_____ Directory server port #: _____ Root bind DN for Oracle Access Manager:_____ Root password:_____ Searchbase:_____ Configuration base:_____ Directory server security mode: _____Open or _____SSL If SSL: ▪ Path to CA Certificate File_____ ▪ Keystore Password_____ Disjoint searchbase:_____
	1.3	Directory Server Profiles (for more information, see specific worksheets for each) _____ _____ _____ _____ _____
	1.4	Master/replica configuration details: _____ _____ _____ _____
	1.5	Types of data in the directory server (circle all that apply for migration): _____Configuration Data _____Policy Data
	1.6	Person Object Class:_____ Group Object Class:_____ User full name attribute:_____ User login ID attribute:_____ Password attribute:_____
	1.7	User class attribute:
	1.8	User login ID attribute:
	1.9	Password attribute:

Worksheet for DIT and Object Definition Details

Use the space in Table A–3 to record details you need for each LDAP directory instance.

Table A–3 DIT and Object Definition Details

Task	Subtask	DIT and Object Definition Details
2	2.1	Directory server DNS host name or IP address:_____ Directory server port #: _____
	2.2	DIT and schema objects used in Oracle Access Manager (or Oracle COREid Release 7.0.4) Person:_____ _____ _____ _____ Group:_____ _____ _____ _____ Others:_____ _____ _____ _____ Diagram DIT (up to 4-level deep):_____ _____ _____ _____ _____
	2.3	Object definition details for all objects managed through Oracle Access Manager: Person:_____ _____ _____ _____ Group:_____ _____ _____ _____ Others:_____ _____ _____ _____ _____ _____

Worksheet for Directory Server Profiles

Use the space in Table A–4 to record details each directory server profile. Consider printing this information from your existing installation.

Table A–4 Details for Directory Server Profiles for Oracle Access Manager/Oracle COREid Release 7.0.4

Task	Subtask	Directory Server Profile Details
3	3.1	Directory server DNS hostname/IP address:_____ Directory server port #: _____
	3.2	Directory Server Profile Profile Name:_____ Namespace (searchbase): _____ Directory Type:_____ Dynamic Auxiliary Classes:_____
	3.3	Operations (circle all that apply) Search Operations:_____Search Entries _____Authenticate Users Read Operations: _____Read Entry Write Operations: ____Create Entry___Modify Entry____Delete Entry____Change Password
	3.4	Used by components (record all that apply) All Identity Servers:_____ _____ _____ Access Servers:_____ _____ _____ Policy Managers (formerly Access Managers):_____ _____ _____
	3.5	Write Operations: _____ Create Entry_____Modify Entry_____Delete Entry Change Password
	3.6	Database Instances (for more information, see specific worksheets for each): _____ _____ _____ _____ _____ _____ _____ _____
	3.7	Maximum Active Servers:_____ Failover Threshold:_____ Sleep for seconds:_____ Max. Session Time (minutes):_____

Worksheet for Database Instance Profiles

Use the space in Table A–5 to record details about each database instance profile associated with a directory server instance. Consider printing this information from your existing installation.

Table A–5 Details for DB Instance Profiles

Task	Subtask	DB Instance Profile Details
4	**4.1**	Directory Server Instance Name:_____ computer Name hosting the directory instance:_____ Port Number: _____ Root DN:_____ Root DN Password:_____ Time Limit:_____ Size Limit:_____ Flags:_____SSL _____Referral_____Fast Bind (AD only) If SSL: ▪ Path to CA Certificate File:_____ ▪ Keystore Password:_____ Secure Port Number:_____ Initial Connections:_____ Maximum Connections:_____

Worksheet for Identity Servers

Use the space in Table A–6 to record details about each Identity Server.

Table A–6 Details for Existing Identity Servers

Task	Subtask	Existing Identity Server Details
5		**Prepare for Identity Configuration Data Migration in Deployment:** Total Number of Identity Servers in this deployment:
	5.1	**Identity Server Details** Installation directory of this Identity Server:_____ Exact Patch Level:_____ Operating System and Patch Level:_____ Installation directory for the associated WebPass:_____
	5.2	Transport security mode between the Identity Server and WebPass: _____Open _____Simple _____Cert If Simple, enter Pass Phrase:_____ If Cert mode, specify full path to: ▪ Certificate file (ois_cert.pem):_____ ▪ Certificate PEM pass phrase:_____ ▪ Key file (ois_key.pem): _____ ▪ Chain file (ois_chain.pem):_____
	5.3	Unique Identity Server ID of this instance:_____ Host name of computer where Identity Server installed:_____ Port number for Identity Server/WebPass communication:_____
	5.4	Directory server type:_____ For more information for this Directory Instance, see worksheet:_____
	5.5	Security mode between directory server and Identity Server: _____SSL _____Open If SSL, path to the Root CA certificate:_____
	5.6	(**Windows only**) Unique Identity Server service name that differentiates this instance in the Services window if you have multiple instances):
	5.7	Auditing configuration: _____ _____
	5.8	Password policy configuration: _____

Worksheet for Policy Manager (release 7.0.4 Access Manager) Instances

Use the space in Table A–7 to record details about each existing Policy Manager (formerly known as the Access Manager component).

Table A–7 Details for Existing Policy Managers

Task	Subtask	Existing Policy Manager Details
6		**Prepare for Policy Data Migration in Deployment:** Total Number of Policy Managers in this deployment:
	6.1	**Policy Manager Instance Details** Installation directory of this Instance _____
	6.2	Is this the master Policy Manager for the data migration? _____Yes _____No Where is policy data stored? - User data directory server - Configuration data directory server - Separate directory server Directory server type_____ _____ Searchbase where user data is stored:_____ Configuration DN:_____ Policy base:_____ For more information for this Directory Instance, see worksheet____ _____
		If the security mode between the directory server and the Policy Manager is SSL, the path to the SSL certificate is:_____
	6.3	Person object class name:
	6.4	Policy Manager policy domain root:

Table A–7 (Cont.) Details for Existing Policy Managers

Task	Subtask	Existing Policy Manager Details
	6.5	Configured Oracle Access Manager 10*g* (10.1.4.0.1)/Oracle COREid Release 7.0.4 authentication schemes? Yes No If Yes, select authentication scheme or schemes: **10*g* (10.1.4.0.1) Authentication Schemes _____ or _____ release 7.0.4 Authentication Schemes** _____Basic Over LDAP_____or_____Basic Over LDAP _____Client Certificate_____or_____Client Certificate _____Anonymous_____or_____NetPoint None Authentication _____Oracle Access and Identity Basic Over LDAP _____or_____NetPoint Basic Over LDAP _____Oracle Access and Identity Basic Over LDAP for AD Forests _____or_____NetPoint Basic Over LDAP for AD Forests - Others _____
	6.6	Configured Oracle Access Manager 10*g* (10.1.4.0.1)/Oracle COREid Release 7.0.4-related policy domains? Yes No If Yes, select policy domains: **10*g* (10.1.4.0.1) Policy Domains** _____or_____ release 7.0.4 Policy Domains _____Identity Domain (a default)_____or_____NetPoint Identity Domain _____Access Domain (a default)_____or_____NetPoint Access Manager Others _____
	6.7	Configured policies to protect Oracle Access Manager 10*g* (10.1.4.0.1) or Oracle COREid Release 7.0.4-related URLs? _____Yes or _____No Details_____

Worksheet for Access Servers

Use the space in Table A–8 to record details about each earlier Access Server. Consider printing some of this information from the Access System Console.

Table A–8 Details for Existing Access Servers

Task	Subtask	Access Server Details
7		**Access Server Details** Total number of Access Servers
	7.1	**Access Server Instance Details** Installation directory of this Access Server Instance _____
	7.2	**Access Server Details in the System Console** Access Server name_____ Access Server host name_____ Port # the Access Server listens to_____ Transport security between Access Server and associated WebGate: ___Open___Simple__Cert Associated WebGate ID_____ Access Management flag: _____ On _____Off
	7.3	Which directory server stores the configuration data? Same as Policy Manager directory server?_____Yes_____No Configuration DN_____ If no, see worksheet for directory server instance_____ Host computer:_____ Port number:_____ Root DN:_____ Root DN password:_____ Directory type:_____ Security mode between the configuration data directory server and the Access Server: _____Open_____SSL
	7.4	Which directory server stores the policy data?_____ Policy base:_____ For more details about directory server instance, see worksheet for_____
	7.5	Transport Security for Access System Components: _____Open_____Simple_____Cert
		Simple mode only: Global Access Protocol pass phrase:_____ Password file:_____
		Cert mode only: Certificate PEM phrase:_____ Password file:_____ Path of the certificate file:_____ Path of the key file:_____ Path of the chain file:_____

Worksheet for Configurations

Use the space in Table A–9 to record details about each configuration.

Table A–9 Details for Existing Configurations

Task	Subtask	Details of Existing Configurations
8	8.1	Installation directory of the configuration: _____ Other components on this computer?_____Yes_____No _____Identity Server_____WebPass_____Policy Manager_____Access Server_____WebGate
	8.2	Workflows: _____ _____ _____ _____
	8.3	User cache flush configuration:_____ AccessGate ID:_____
	8.4	Access Control Lists (ACLs): _____ _____ _____
	8.5	Custom Identity Event plug-ins (workflow details involving this plug-in, pre- or post actions) **Plug-in Name**:_____ Workflow Details:_____ Pre-event Actions:_____ Post-event Actions:_____ **Plug-in Name**:_____ Workflow Details:_____ Pre-event Actions:_____ Post-event Actions:_____ **Plug-in Name**:_____ Workflow Details:_____ Pre-event Actions:_____ Post-event Actions:_____ **Plug-in Name**:_____ Workflow Details:_____ Pre-event Actions:_____ Post-event Actions:_____ **Plug-in Name**:_____ Workflow Details:_____ Pre-event Actions:_____ Post-event Actions:_____

Table A–9 (Cont.) Details for Existing Configurations

Task	Subtask	Details of Existing Configurations
	8.6	Customized Authentication plug-ins: _____
	8.7	Customized Authorization plug-ins: _____
	8.8	10*g* (10.1.4.0.1) Access Manager API clients/release 7.0.4 Access Server API clients:

Checklist for Deploying and Setting Up the Configuration Manager

Use the checklist in Table A–10 to track the progress of "Deploying and Setting Up the Configuration Manager".

Table A–10 Checklist for Schema and Data Preparation

Done	Checklist for Deploying and Setting Up the Configuration Manager
	Deployment Name:_____ **Task owner**:_____
	Planning for Configuration Manager Deployment on page 2-1
	Setting Up a Repository and Installing OC4J on page 2-5 Installing and Setting up the Oracle Database Repository on page 2-6 Installing and Configuring OC4J on page 2-7
	Deploying the Configuration Manager on page 2-12
	Assigning Configuration Manager Administrator and User Roles in OC4J on page 2-16
	Adding Repository Details in the Configuration Manager on page 2-29
	Ensuring the Repository is Available to the Configuration Manager on page 2-32

Checklist for Configuration Data Migration

Use the checklist in Table A–11 to track the progress of migrating data changes. This checklist should be used in conjunction with the information in chapters noted in the table.

Table A–11 Checklist for Configuration Data Migration

Done	Checklist for Configuration Data Migration
	Deployment Name:_____ **Task owner**:_____
	Notifying Other Administrators on page 3-3
	Adding Environment Details to the Configuration Manager on page 3-5
	Creating a Directory Association on page 3-15
	Adding and Managing Optional Transformation Rules on page 3-31
	Creating a Snapshot on page 3-39
	Migrating Data from the Source to the Target on page 3-43 **See also**: " Data to Migrate Using Another Tool" on page A-15.
	Restarting Servers After Migration on page 3-55
	Validating Migration Success on page 4-1
	Rolling Back Changes Made During a Specific Transaction on page 5-3 Transaction ID:_____ Date of Roll back:_____ Reason for Roll back:_____
	Restoring the Content of a Snapshot on page 5-9 SnapShot ID:_____ Date of Restoration:_____ Reason for Restoration:_____

Checklist for Migration of Other Data Using Another Tool

Oracle Access Manager Configuration Manager migrates only data in the LDAP directory. It does **not** migrate any files.

The items in Table A–12 are not supported for migration using Oracle Access Manager Configuration Manager. To migrate data in Table A–12, you must use other code management products for check in, check out, and deployment. Details of other tools are outside the scope of this manual.

Table A–12 Data to Migrate Using Another Tool

Done	Description
	Data that **cannot** be migrated using Oracle Access Manager Configuration Manager: Data Type_____Tool Used to Migrate This Data:_____ ■ PPP catalog (and associated called scripts/code) _____ ■ Javascript _____ ■ Images _____ ■ Stylesheets _____ ■ Authentication Plug-in Code (if any) _____ ■ Authorization Plug-in Code (if any) _____

B

Troubleshooting Configuration Manager Issues

The information here is provided to help you when troubleshooting issues that arise during installation and setup of Oracle Access Manager Configuration Manager and data migration. Secrtions in this chapter include:

Accessing and Using the Log File

As mentioned in Chapter 2, Oracle Access Manager Configuration Manager uses Oracle Diagnostic Logging for Java (ODL) to produce log files.

The generated log file helps administrators verify Configuration Manager activities such as adding a new environment, creating snapshots, migrating data, and so on. Log entries include details about Oracle Access Manager Configuration Manager, the repository, and environments (directory servers). For example, if you attempt to add new environment (LDAP directory) details in Configuration Manager when the repository is offline, a log entry is created stating that the database is not running.

Log File Naming: The current ODL log file naming standard is followe, which means that each new log file that is generated is named log.xml. The generated log file is stored as:

$*OC4J_Home*/j2ee/home/log/OAMCMLogs/log.xml

You configure logs for Oracle Access Manager Configuration Manager by including specific logger and log handler details in the in the following file:

OC4J_Home/j2ee/home/config/j2ee-logging.xml

The following sample j2ee-logging.xml file does not include any details for Oracle Access Manager Configuration Manager:

```
<?xml version="1.0" encoding="iso-8859-1?>
<!-- Logging configuration file for OC4J.  The guidelines are based on the
java.util.logging package and the DTD for this XML file can be found
in the javadoc for oracle.core.ojdl.logging.LoggingConfiguration on
```

```
http://dms.us.oracle.com/javadoc/ -->
<logging_configuration>
  <log_handlers>
    <log_handler name="console-handler"
      class="java.util.logging.ConsoleHandler"
      formatter="oracle.core.ojdl.logging.SimpleFormatter"/>
    <log_handler name="oc4j-handler"
      class="oracle.core.ojdl.logging.ODLHandlerFactory">
      <property name="path" value="../log/oc4j"/>
      <property name="maxFileSize" value="10485760"/>
      <property name="maxLogSize" value="104857600"/>
      <property name="encoding" value="UTF-8"/>
    </log_handler>
  </log_handlers>
<loggers>
<!-- Default Logger, useParentHandlers should be set to false because
the root Logger (named the empty string "") will log to console -->
   <logger name="oracle" level="NOTIFICATION:1"
     useParentHandlers="false">
     <handler name="oc4j-handler"/>
     <handler name="console-handler"/>
   </logger>
 </loggers>
</logging_configuration>
```

The following sample j2ee-logging.xml file includes the encoding, logger, and log handler entries (in **bold**, based on ODL specifications) that are required to enable logging for Oracle Access Manager Configuration Manager. For the steps to edit this file, see "Configuring Logging for Oracle Access Manager Configuration Manager" on page 2-33.

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- Logging configuration file for OC4J.  The guidelines are based on the
java.util.logging package and the DTD for this XML file can be found
in the javadoc for oracle.core.ojdl.logging.LoggingConfiguration on
http://dms.us.oracle.com/javadoc/ -->
<logging_configuration>
  <log_handlers>
    <log_handler name="console-handler"
      class="java.util.logging.ConsoleHandler"
      formatter="oracle.core.ojdl.logging.SimpleFormatter"/>
    <log_handler name="oc4j-handler"
      class="oracle.core.ojdl.logging.ODLHandlerFactory">
      <property name="path" value="../log/oc4j"/>
      <property name="maxFileSize" value="10485760"/>
      <property name="maxLogSize" value="104857600"/>
      <property name="encoding" value="UTF-8"/>
    </log_handler>
    <!-HM Application specific log Handler -->
  <log_handlername="HMLog-Handler"
    class="oracle.core.ojdl.logging.ODLHandlerFactory">
      <property name="path" value="../log/OAMCMLogs"/>
      <property name="maxFileSize" value="10485760"/>
      <property name="maxLogSize" value="104857600"/>
      <property name="encoding" value="UTF-8"/>
  </log_handler>
 </log_handlers>
<loggers>
  <!-- Default Logger, useParentHandlers should be set to false because
  the root Logger (named the empty string "") will log to console -->
```

```
      <logger name="oracle" level="NOTIFICATION:1"
        useParentHandlers="false">
        <handler name="oc4j-handler"/>
        <handler name="console-handler"/>
      </logger>
      <!-- HM Application logger -->
     <logger name="com.oracle.hm.log.HMLogger" level="ALL"
       useParentHandlers="false">
       <handler name="HMLog-Handler"/>
     </logger>
    </loggers>
   </logging_configuration>
```

Generated Log File Content and Logging Levels

The generated log file includes the operation name, the individual who performed the operation, a time stamp, the status of the operation, and any errors as discussed later. J2SE includes two standard formatters:

- SimpleFormatter: Writes brief human-readable summaries of log records.
- XMLFormatter: Writes detailed XML-structured information.

You can either view the generated log file as an XML file or apply a stylesheet of your own design to view the files. Oracle Access Manager Configuration Manager does not provide stylesheets for this purpose.

Normal event information is provided to administrators. Low-level traces and debug information can be provided to advanced administrators. For details about specific events and who can view these, see Table B–4.

The log file looks something like the following example:

```
<MESSAGE>
  <HEADER>
    <TSTZ_ORIGINATING>2006-07-20T18:57:17.968+05:30</TSTZ_ORIGINATING>
    <COMPONENT_ID>oracle</COMPONENT_ID>
    <MSG_TYPE"NOTIFICATION"></MSG_TYPE>
    <MSG_LEVEL>1</MSG_LEVEL>
    <HOST_ID>ps0065</HOST_ID>
    <HOST_NWADDR>10.77.199.149</HOST_NWADDR>
    <MODULE_ID>hm.log.HMLogger</MODULE_ID>
    <THREAD_ID>10</THREAD_ID>
    <USER_ID>sharadchandra_chaval</USER_ID>
  </HEADER>
  <CORRELATION_DATA>

<EXEC_CONTEXT_ID><UNIQUE_ID>10.77.199.149:25178:1153402038031:0</UNIQUE_
ID><SEQ>0</SEQ></EXEC_CONTEXT_ID>
  </CORRELATION_DATA>
  <PAYLOAD>
    <MSG_TEXT>Entering Into Method - com.oracle.hm.hmobjectshandler.
     HMObjectsHandler.getInstance </MSG_TEXT>
  </PAYLOAD>
</MESSAGE>
....
<MESSAGE>
  <HEADER>
    <TSTZ_ORIGINATING>2006-07-20T18:57:18.062+05:30</TSTZ_ORIGINATING>
    <COMPONENT_ID>oracle</COMPONENT_ID>
```

```
    <MSG_TYPE TYPE="NOTIFICATION"></MSG_TYPE>
    <MSG_LEVEL>1</MSG_LEVEL>
    <HOST_ID>ps0065</HOST_ID>
    <HOST_NWADDR>10.77.199.149</HOST_NWADDR>
    <MODULE_ID>hm.log.HMLogger</MODULE_ID>
    <THREAD_ID>10</THREAD_ID>
    <USER_ID>gail_tiberi</USER_ID>
  </HEADER>
```

Each log message contains a number of required attributes, and can contain additional optional attributes.

Required Attributes: All diagnostics log messages must have the following attributes:

- Time stamp
- Component ID
- Message type
- Message ID (for each message of the type Notification and greater)
- Execution Context ID
- Message level
- Message text
- Module ID (use the component ID if the component is a single module component)

Optional Attributes: Diagnostics log messages can have the following attributes:

- Organization ID
- Instance ID
- User ID
- Message Arguments
- Process ID
- Thread ID
- Host ID
- Host Network Address
- Supplemental Detail

> **Note:** The Logging Service will be able to provide the Instance ID, Process ID, Host ID, and Host Network Address. Avoid using implicit attributes.

Component-Specific Attributes: Components might have additional component-specific attributes that are added using the supplemental attributes fields. The definition and contents of these attributes are specific to each component. For supplemental, Oracle Enterprise Manager requires user-friendly names (WIP, for example).

Implicit Attributes: The value of some attributes might be implicit from the context, even if it does not appear explicitly in the log message. For example, if a component has a private log that only contains log messages for that component (for example, a log for OC4J that has messages only for that OC4J instance), then all log messages are

assumed to have the component ID attribute set to the component that owns the log. Avoid using implicit attributes.

Table B–1 provides more information about ODL log message text format fields.

Table B–1 ODL Log Message Text Format Fields

Field Name	Short Name	Required (Y/N)	Comments
TIMESTAMP, ORIGINATING	N/A	Y	Use [] if no value
TIMESTAMP, NORMALIZED	N/A	N	Use [] if no value
COMPONENT ID	N/A	Y	Use [] if no value
MESSAGE ID	N/A	Y	Use [] if no value
MESSAGE TYPE	N/A	Y	Use [] if no value
MESSAGE LEVEL	N/A	Y	Use [] if no value
MODULE ID	N/A	Y	
MESSAGE TEXT	N/A	Y	
EXECUTION_CONTEXT_ID	ecid	Y	
ORGANIZATION_ID	org	N	
HOSTING_CLIENT_ID	hostingClientid	N	
MESSAGE_GROUP	group	N	
HOST_ID	host	N	
HOST_NWADDR	nwaddr	N	
PROCESS_ID		N	
THREAD_ID	tid	N	
USER_ID	userid	N	
UPSTREAM_COMPONENT_ID	upstreamComp	N	
DOWNSTREAM_COMPONENT_ID	downstreamComp	N	
ERROR_INSTANCE_ID	errid	N	
DETAIL_LOCATION	detailLoc	N	

Table B–2 outlines the diagnostic message attributes in more detail.

Table B–2 Log File Diagnostic Message Attributes

Attribute Name	Description	Example
Timestamp, originating	Date and time when the message was generated. The timestamp should have as much precision as possible. At a minimum is should it should have at least up to the second, but using milliseconds is recommended.	2003-12-20T12:30:45.123-08:00
Timestamp, normalized	Date and time when the message was generated, adjusted for time difference between the host where the message was generated and the host of the common repository. This field is only set when the log message is written to a central repository, and should not be set by components.	2003-12-20T12:30:45.123-08:00
Organization ID	The organization that wrote the component that originated the message. All Oracle components should use '`oracle`'.	oracle
Component ID	The component that originated the message.	OHS
Instance ID	The instance to which the component that originates the messages belongs. This field will usually be set only when messages are written to a central repository.	OraHome1.mjgoncal-sun.us.oracle.com

Table B–2 (Cont.) Log File Diagnostic Message Attributes

Attribute Name	Description	Example
Message ID	A short identifier that uniquely identifies the message. The Message ID should be in the format *<component prefix>-<message number>*, where *<component prefix>* is a short component prefix (a six character maximum) and *<message number>* is a five digit number.	MAS-12345
Message Type	The type of the message. The five defined message types are: INTERNAL_ERROR, ERROR, WARNING, NOTIFICATION, and TRACE. In addition, the value UNKNOWN can be used when the type is not known.	NOTIFICATION
Message Level	The level qualifies the message type, indicating the degree of severity of the message. The value is an integer from 1 (highest severity) to 32 (lowest severity).	1
Host ID	The host name where the message originates. For Java, this should be the value returned by java.net.InetAddress.getLocalHost().getHostName().	mjgoncal-sun.us.oracle.com
Host NW Addr	The network address of the host where the message originates. For Java, this should be the value returned by java.net.InetAddress.getLocalHost().getHostAddress().	138.1.42.113
Module ID	An identifier of the module that originated the message. The value is component specific	main
Process ID	An identifier of the process or execution unit that generated the message. The value should be the operating system PID, or some other value that can be used to identify the process.	1234
Thread ID	An identifier of the thread that generated the messages	main
User ID	The user whose execution context originated the message	scott
Supplemental Attributes	A list of supplemental, application specific, message attributes. Each supplemental attribute must have a name and value	name=URL, value=/dmsoc4j/Spy
Execution Context ID	A global unique identifier and a sequence number of the thread of execution that the originating component participates in. The identifier can be used to correlate messages from several components that can be involved in the same thread of execution.	1234567890,1
Message Text	A descriptive text for the message. This should be a short description of the event, with at most 1000 characters.	
Supplemental Detail	Supplemental information about the event. This can contain more detailed information than the message text. A Java stack trace, for example, should be in the supplemental detail, not in the message text.	java.lang.NullPointerExceptio n at Test.main(Test.java:20)

Logging Levels and Message Types

In `java.util.logging`, levels are represented by objects of class `java.util.logging.Level`. There is a small number of predefined levels (`SEVERE, WARNING, INFO, CONFIG, FINE, FINER, FINEST`). However, applications can create additional levels. Each level is uniquely identified by an integer value. Therefore, it is possible to create one new level object for each possible integer value.

Java levels are mapped to ODL message types and levels. In general, only the ODL message types and levels should be exposed in the component configuration. Mapping of ODL message type and level to `java.util.logging.Level` will be provided by a subclass of the Level class. All possible Java levels (from `Integer.MIN_VALUE` to `Integer.MAX_VALUE`) have a mapping. Components are not restricted to using the predefined levels. The mapping for the predefined java levels as shown in Table B–3

Table B–3 Java Levels and Corresponding ODL MessageType:Level

Java Level	ODL MessageType:Level
SEVERE.intValue()+100	INTERNAL_ERROR:1
SEVERE	ERROR:1
WARNING	WARNING:1
INFO	NOTIFICATION:1
CONFIG	NOTIFICATION:16
FINE	TRACE:1
FINER	TRACE:1
FINEST	TRACE:32

Java levels with an integer value that falls between two predefined levels are mapped to the next mapped MessageType (with the ODL level set to an appropriate value), depending on the difference between the level and the next predefined level. Java levels less than FINEST and greater than SEVERE.intValue() + 100 are mapped to UNKNOWN.

Messages of type INTERNAL_ERROR, ERROR, WARNING and NOTIFICATION have a message ID composed of a short component prefix (3 to 6 characters) and a 5-digit message number. For example, MAS-12345.

Table B–4 outlines the log file message types and levels in greater detail.

Table B–4 Log File Message Types

ODL Message Type/Level (Java Level)	Intended Audience	Description	Expected Volume
INTERNAL_ERROR:1 (SEVERE.intValue()+100)	System Administrators, Application Developers, Oracle Support	A serious problem that can be caused by a bug in the product and that should be reported to Oracle Support. The occurrence of an internal error triggers the generation of an incident by the Diagnosability Framework.	Low. No performance impact.
ERROR:1 (SEVERE)	System Administrators Application Developers, Oracle Support	A serious problem that requires immediate attention from the System Administrator. This is *not* caused by a bug in the product	Low. No performance impact.
WARNING:1 (WARNING)	System Administrators Application Developers, Oracle Support	A potential problem that should be reviewed by the System Administrator.	Low. No performance impact.
NOTIFICATION:1 (INFO)	System Administrators Application Developers, Oracle Support	A normal event that occurs in the System. No performance impact. This is the default Level at which the product is shipped.	Low
NOTIFICATION:16 (CONFIG)	System Administrators Application Developers, Oracle Support	A finer level of granularity for reporting normal events. Minimal performance impact. While this is not the default Level for the product, it should be possible to enable this level broadly in a production environment without having a significant performance impact in the product.	Low to moderate.

Table B–4 (Cont.) Log File Message Types

ODL Message Type/Level (Java Level)	Intended Audience	Description	Expected Volume
TRACE:1 (FINE)	Advanced System Administrators, Advanced Application Developers, Oracle Support	Trace or debug information for events that are meaningful to end users of the product, such as public API entry/exit points. The messages should be clear enough to be understood by someone who does not know internal implementation details. Small performance impact. This level can be enabled broadly occasionally on a production environment to debug issues with the product. Enabling logging at this level can have a small performance impact, but not to the point of making the product unusable. It should be possible to enable this level on a production system to write to a circular memory buffer (MemoryHandler) without a significant performance impact	Moderate
TRACE:16 (FINER)	Oracle Support	Detailed trace or debug information that can help Oracle Support diagnose problems with a particular subsystem. The messages should be clear enough to be understood by Oracle Support engineers who have a deep knowledge of the product but cannot know full details of the internal implementation. This level should not be enabled on a production environment, except on special situations to debug issues with the product. It is not expected that this level will be enabled broadly for the product, but only for a few specific sub-systems (loggers).	High
TRACE:32(FINEST)	Oracle DDR	Very detailed trace or debug information that usually is intended for an Oracle developer working on the product and who knows enough details about the implementation of the sub-system that generates the message. This level is not expected to be enabled in a production environment and it is intended to be used to debug the product on a test or development environment	Very high

Accessing and Using the Audit File

Oracle Access Manager Configuration Manager audits certain events and stores all audit entries in the Oracle Database repository, in the OCMAUDIT table. You can query the OCMAUDIT table within the Oracle Database repository and use external applications to view these reports.

Oracle Access Manager Configuration Manager audits the event types for the functions outlined in Table B–5.

Table B–5 Audited Event Types and Functions

	Read/ Access	Write/ Add/ Create	Update	Delete	Restore
Environment Functions		Y	Y	Y	
Association Functions		Y	Y	Y	
Transformation_Rule Functions		Y	Y	Y	

Table B–5 (Cont.) Audited Event Types and Functions

	Read/ Access	Write/ Add/ Create	Update	Delete	Restore
Snapshot Functions		Y		Y	Y
Transaction Functions		Y	Y	Y	
Database Configuration Functions			Y		

A report is generated by exporting the Oracle Access Manager Configuration Manager audit table from the Oracle Database repository to a Microsoft Excel spreadsheet. You can use Crystal Reports to view an audit report of your own configuration.

To create an audit report

1. Query the OCMAUDIT table in the Oracle Database repository.
2. Export the OCMAUDIT table into a spreadsheet application.
3. Use an external reporting tool (Crystal Reports) to view the report.

Table B–6 shows a sample audit report from Oracle Access Manager Configuration Manager.

Table B–6 Sample Audit Report

COMPONENT_ NAME	EVENT_ TYPE	EVENT_ OWNER	EVENT_DATETIME	EVENT_ STATUS	EVENT_DESCRIPTION
Snapshot	Create	User_A	Fri Nov 03 13:50:07 GMT+05:30 2006	Successful	Create Snapshot SnapshotName=TestSnaphot, EnvironmentName=10104DEV
Snapshot	Restore	User_A	Fri Nov 03 13:51:23 GMT+05:30 2006	Successful	Create Snapshot SnapshotName=TestSnaphot, EnvironmentName=10104DEV
Snapshot	Restore	User_A	Fri Nov 03 13:51:36 GMT+05:30 2006	Successful	Create Snapshot SnapshotName=TestSnaphot, EnvironmentName=10104DEV
Database_ Configuration	Update	Admin_A	Fri Nov 03 13:53:16 GMT+05:30 2006	Successful	Update Database_Configuration
Environment	Create	User_B	Fri Nov 03 14:07:40 GMT+05:30 2006	Successful	Create: EnvironmentName=TestAudit
Environment	Create	User_B	Fri Nov 03 14:07:41 GMT+05:30 2006	Successful	Add Environment Parameter : EnvironmentName=TestAudit, Parameter : password=TestAudit
Environment	Create	User_B	Fri Nov 03 14:07:41 GMT+05:30 2006	Successful	Add Environment Parameter : EnvironmentName=TestAudit, Parameter : config-dn=TestAudit
Environment	Create	User_B	Fri Nov 03 14:07:41 GMT+05:30 2006	Successful	*Other entries not included in this table.*
Environment	Create	User_B	Fri Nov 03 14:07:41 GMT+05:30 2006	Successful	Add Environment Parameter : EnvironmentName=TestAudit, Parameter : port=1947
Environment	Update	User_B	Fri Nov 03 14:10:38 GMT+05:30 2006	Successful	Update : EnvironmentName=TestAudit, Parameters : Description=TestAuditChanging
Environment	Update	User_B	Fri Nov 03 14:10:40 GMT+05:30 2006	Successful	Update Environment Parameter : EnvironmentName=TestAudit, Parameters : password=TestAudit

Table B–6 (Cont.) Sample Audit Report

COMPONENT_ NAME	EVENT_ TYPE	EVENT_ OWNER	EVENT_DATETIME	EVENT_ STATUS	EVENT_DESCRIPTION
Environment	Update	User_B	Fri Nov 03 14:10:40 GMT+05:30 2006	Successful	Update Environment Parameter : EnvironmentName=TestAudit, Parameters : config-dn=TestAudit
Environment	Update	User_B	Fri Nov 03 14:10:40 GMT+05:30 2006	Successful	Update Environment Parameter : EnvironmentName=TestAudit, Parameters : hostName=TestAudit
Environment	Update	User_B	Fri Nov 03 14:10:40 GMT+05:30 2006	Successful	*Other entries not included in this table.*
Environment	Delete	User_B	Fri Nov 03 14:11:23 GMT+05:30 2006	Successful	Delete Environment Parameters : EnvironmentName=TestAudit
Association	Create	User_A	Fri Nov 03 14:13:39 GMT+05:30 2006	Successful	Create : AssociationName=TestAuditAssociation
Association	Update	User_A	Fri Nov 03 14:13:39 GMT+05:30 2006	Successful	Update : AssociationName=TestAuditAssociation
Transformation_ rule	Delete	User_A	Fri Nov 03 14:14:49 GMT+05:30 2006	Successful	Delete Transformation Rules For Association : AssociationName=TestAuditAssociation
Association	Delete	User_A	Fri Nov 03 14:13:39 GMT+05:30 2006	Successful	Delete : AssociationName=TestAuditAssociation
Transaction	Create	User_A	Fri Nov 03 14:19:14 GMT+05:30 2006	Successful	Started Transaction TransactionID=2114, AssociationName=1014Dev-QA
Transaction	Update	User_A	Fri Nov 03 14:19:14 GMT+05:30 2006	Successful	Update Transaction Status : TransactionID=2114
Transaction	Commit	User_A	Fri Nov 03 14:19:23 GMT+05:30 2006	Successful	Commit Transaction : TransactionID=2114

Message, Cause, Resolution

Table B–7provides a list of messages that you might see as well as the cause of the message and actions that you can take the resolve the issue

Table B–7 Configuration Manager Message, Cause, and Resolution

Number	Message	Cause	Resolution
1	OAMCM application repository is not configured or not running	1. The repository is down or offline. 2. Repository details on the Configuration Manager System Configuration tab might be inaccurate or incomplete.	Perform the following steps, as needed: 1. Test the repository connection from the System Configuration tab. See "Ensuring the Repository is Available to the Configuration Manager" on page 2-32. 2. If the connection test fails, ensure that repository is live and online. 3. If repository is live and online, ensure that the repository details on the Configuration Manager System Configuration tab are complete and accurate. See "Adding Repository Details in the Configuration Manager" on page 2-29
2	Environment Parameter Not Found - config-DN	The configuration DN parameter for the LDAP directory environment was not found in the repository. If environment information was entered, it might be inaccurate or incomplete or the configuration DN might not start from the `oblix` node.	1. Confirm that environment details are complete and accurate. See "Adding and Managing Environment Details in the Configuration Manager" on page 3-4. 2. Confirm that the configuration DN starts from the `oblix` node.
3	Environment Parameters Found NULL	The environment parameters could not be found. 1. The repository is down or offline. 2. Repository details on the Configuration Manager System Configuration tab might be inaccurate or incomplete.	Perform the following steps, as needed: 1. Test the repository connection from the System Configuration tab. See "Ensuring the Repository is Available to the Configuration Manager" on page 2-32. 2. If the connection test fails, ensure that repository is live and online. 3. If the repository is live and online, ensure that the repository details on the Configuration Manager System Configuration tab are complete and accurate. See "Adding Repository Details in the Configuration Manager" on page 2-29
4	Logical Object Is NULL	Oracle Access Manager Configuration Manager failed to fetch the logical object from the LDAP directory environment. Perhaps the LDAP directory environment is down.	Perform the following steps, as needed: 1. Cancel the Migration operation. 2. Click the Test Environment button to ensure that this directory is live and online. See "Testing the Environment Connection" on page 3-12 3. Start migrating data again. See "Migrating Data" on page 3-51.
5	Error In Getting Database Processor.	This Oracle Database processor-related exception occurs mainly when the Configuration Manager cannot connect to the repository. This might mean that: 1. The repository is down or offline. 2. Repository details on the Configuration Manager System Configuration tab might be inaccurate or incomplete.	Perform the following steps, as needed: 1. Test the repository connection from the System Configuration tab. See "Ensuring the Repository is Available to the Configuration Manager" on page 2-32. 2. If the connection test fails, ensure that repository is live and online. 3. If the repository is live and online, ensure that the repository details on the Configuration Manager System Configuration tab are complete and accurate. See "Adding Repository Details in the Configuration Manager" on page 2-29

Table B–7 (Cont.) Configuration Manager Message, Cause, and Resolution

Number	Message	Cause	Resolution
6	Failed To Get Environment Using Database Processor.	This Oracle Database processor-related exception occurs mainly when the Configuration Manager cannot connect to the repository. This might mean that: 1. The repository is down or offline. 2. Repository details on the Configuration Manager System Configuration tab might be inaccurate or incomplete.	Perform the following steps, as needed: 1. Test the repository connection from the System Configuration tab. See "Ensuring the Repository is Available to the Configuration Manager" on page 2-32. 2. If the connection test fails, ensure that the repository is live and online. 3. If the repository is live and online, ensure that the repository details on the Configuration Manager System Configuration tab are complete and accurate. See "Adding Repository Details in the Configuration Manager" on page 2-29 4. If repository details are complete and accurate, click the Test Environment button to ensure that this directory is live and online. See "Testing the Environment Connection" on page 3-12 5. If the environment connection is successful but you still cannot reach the environment, ensure that the LDAP directory is online and that the environment details are complete and accurate. See "Adding and Managing Environment Details in the Configuration Manager" on page 3-4.
7	Failed To Get Environment - HMEnvironmentCreationException Found.	Either the repository is not accessible or the LDAP directory environment is not accessible.	Perform the following steps, as needed: 1. Test the repository connection from the System Configuration tab. See "Ensuring the Repository is Available to the Configuration Manager" on page 2-32. 2. If the connection test fails, ensure that repository is live and online. 3. If the repository is live and online, ensure that the repository details on the Configuration Manager System Configuration tab are complete and accurate. See "Adding Repository Details in the Configuration Manager" on page 2-29. 4. If repository details are complete and accurate, click the Test Environment button to ensure that this directory is live and online. See "Testing the Environment Connection" on page 3-12 5. If the environment connection is successful but you still cannot reach the environment, ensure that the LDAP directory is online and that the environment details are complete and accurate. See "Adding and Managing Environment Details in the Configuration Manager" on page 3-4.

Table B–7 (Cont.) Configuration Manager Message, Cause, and Resolution

Number	Message	Cause	Resolution
8	Failed To Get Environment	Either the repository is not accessible or the LDAP directory environment is not accessible.	Perform the following steps, as needed: 1. Test the repository connection from the System Configuration tab. See "Ensuring the Repository is Available to the Configuration Manager" on page 2-32. 2. If the connection test fails, ensure that the repository is live and online. 3. If the repository is live and online, ensure that the repository details on the Configuration Manager System Configuration tab are complete and accurate. See "Adding Repository Details in the Configuration Manager" on page 2-29. 4. If repository details are complete and accurate, click the Test Environment button to ensure that this directory is live and online. See "Testing the Environment Connection" on page 3-12 5. If the environment connection is successful but you still cannot reach the environment, ensure that the LDAP directory is online and that the environment details are complete and accurate. See "Adding and Managing Environment Details in the Configuration Manager" on page 3-4.
9	Error While Getting Environment LogicalObject IDs	Either the repository is not accessible or the LDAP directory environment is not accessible or the configuration DN is not accessible.	Perform the following steps, as needed: 1. Test the repository connection from the System Configuration tab. See "Ensuring the Repository is Available to the Configuration Manager" on page 2-32. 2. If the connection test fails, ensure that the repository is live and online. 3. If the repository is live and online, ensure that the repository details on the Configuration Manager System Configuration tab are complete and accurate. See "Adding Repository Details in the Configuration Manager" on page 2-29. 4. If repository details are complete and accurate, click the Test Environment button to ensure that this directory is live and online. See "Testing the Environment Connection" on page 3-12 5. If the environment connection is successful but you still cannot reach the environment, ensure that the LDAP directory is online and that the environment details are complete and accurate. See "Adding and Managing Environment Details in the Configuration Manager" on page 3-4. 6. If the LDAP environment details are complete and accurate, ensure that the environment in the deployment is live and online.

Table B–7 (Cont.) Configuration Manager Message, Cause, and Resolution

Number	Message	Cause	Resolution
‘0	SQLException Occurred While Adding Snapshot Entry Into Database	Either the repository is not accessible or the LDAP directory environment is not accessible (the configuration DN is not accessible).	Perform the following steps, as needed: 1. Test the repository connection from the System Configuration tab. See "Ensuring the Repository is Available to the Configuration Manager" on page 2-32. 2. If the connection test fails, ensure that the repository is live and online. 3. If the repository is live and online, ensure that the repository details on the Configuration Manager System Configuration tab are complete and accurate. See "Adding Repository Details in the Configuration Manager" on page 2-29. 4. If repository details are complete and accurate, click the Test Environment button to ensure that this directory is live and online. See "Testing the Environment Connection" on page 3-12 5. If the environment connection is successful but you still cannot reach the configuration DN, ensure that the LDAP directory is online and that the environment details are complete and accurate. See "Adding and Managing Environment Details in the Configuration Manager" on page 3-4.
11	HMRepositortException Occurred While Getting Connection To Database	1. Oracle Database is down or offline. 2. Oracle Database details on the Configuration Manager System Configuration tab might be inaccurate or incomplete.	Perform the following steps, as needed: 1. Test the repository connection from the System Configuration tab. See "Ensuring the Repository is Available to the Configuration Manager" on page 2-32. 2. If the connection test fails, ensure that the repository is live and online. 3. If the repository is live and online, ensure that the repository details on the Configuration Manager System Configuration tab are complete and accurate. See "Adding Repository Details in the Configuration Manager" on page 2-29
12	Snapshot Of Config Data Failed	1. The LDAP directory environment might not be live and online. 2. One node might refer to another node that was removed as the result of an action that occurred outside the Configuration Manager. As a result, the Configuration Manager cannot find the entries. 3. The configuration DN might not start from the `oblix` node.	Perform the following steps, as needed: 1. Click the Test Environment button on the View Environment page to ensure that the directory is live and online. See "Testing the Environment Connection" on page 3-12. 2. Ensure that the LDAP directory environment details are complete and accurate. See "Adding and Managing Environment Details in the Configuration Manager" on page 3-4 3. Confirm that the configuration DN starts from the `oblix` node.

Table B–7 (Cont.) Configuration Manager Message, Cause, and Resolution

Number	Message	Cause	Resolution
13	Snapshot Of Policy Data Failed	1. The LDAP directory environment might not be live and online. 2. One node might refer to another node that was removed as the result of an action that occurred outside the Configuration Manager. As a result, the Configuration Manager cannot find the entries. 3. The configuration DN might not start from the `oblix` node.	Perform the following steps, as needed: 1. Click the Test Environment button on the View Environment page to ensure that the directory is live and online. See "Testing the Environment Connection" on page 3-12. 2. Check the environment directly to ensure that no node has been removed outside the Configuration Manager. 3. Ensure that the LDAP directory environment details are complete and accurate. See "Adding and Managing Environment Details in the Configuration Manager" on page 3-4 4. Confirm that the configuration DN starts from the `oblix` node.
14	Invalid username/password; logon denied.	1. Invalid login credentials. 2. Account locked out (usually due to invalid logon tries exceed the limit).	1. Provide proper credentials to log in. 2. Unlock the Account.
15	Directory Server Connection Failed.	The LDAP directory environment might not be live and online or the environment specifications in the Configuration Manager might be incomplete or inaccurate.	Perform the following steps, as needed: 1. Click the Test Environment button on the View Environment page to ensure that the directory is live and online. See "Testing the Environment Connection" on page 3-12. 2. Ensure that the LDAP directory environment details are complete and accurate. See "Adding and Managing Environment Details in the Configuration Manager" on page 3-4
16	Error Occurred While importing the ldif file into the directory	The LDAP directory environment might not be live and online or the environment specifications in the Configuration Manager might be incomplete or inaccurate.	Perform the following steps, as needed: 1. Click the Test Environment button on the View Environment page to ensure that the directory is live and online. See "Testing the Environment Connection" on page 3-12. 2. Ensure that the LDAP directory environment details are complete and accurate. See "Adding and Managing Environment Details in the Configuration Manager" on page 3-4
17	Database Connection Failed, Connection Object Found NULL	1. The repository is down or offline. 2. Repository details on the Configuration Manager System Configuration tab might be inaccurate or incomplete.	Perform the following steps, as needed: 1. Test the repository connection from the System Configuration tab. See "Ensuring the Repository is Available to the Configuration Manager" on page 2-32. 2. If the connection test fails, ensure that the repository is live and online. 3. If repository is live and online, ensure that the repository details on the Configuration Manager System Configuration tab are complete and accurate. See "Adding Repository Details in the Configuration Manager" on page 2-29

Table B–7 (Cont.) Configuration Manager Message, Cause, and Resolution

Number	Message	Cause	Resolution
18	SQLException - While creating database connection.	1. The repository is down or offline. 2. Repository details on the Configuration Manager System Configuration tab might be inaccurate or incomplete.	Perform the following steps, as needed: 1. Test the repository connection from the System Configuration tab. See "Ensuring the Repository is Available to the Configuration Manager" on page 2-32. 2. If the connection test fails, ensure that the repository is live and online. 3. If repository is live and online, ensure that the repository details on the Configuration Manager System Configuration tab are complete and accurate. See "Adding Repository Details in the Configuration Manager" on page 2-29
19	SQLException - While connection Commit	1. The repository is down or offline. 2. Repository details on the Configuration Manager System Configuration tab might be inaccurate or incomplete.	Perform the following steps, as needed: 1. Test the repository connection from the System Configuration tab. See "Ensuring the Repository is Available to the Configuration Manager" on page 2-32. 2. If the connection test fails, ensure that the repository is live and online. 3. If repository is live and online, ensure that the repository details on the Configuration Manager System Configuration tab are complete and accurate. See "Adding Repository Details in the Configuration Manager" on page 2-29
20	SQLException -While Create Statement	1. The repository is down or offline. 2. Repository details on the Configuration Manager System Configuration tab might be inaccurate or incomplete.	Perform the following steps, as needed: 1. Test the repository connection from the System Configuration tab. See "Ensuring the Repository is Available to the Configuration Manager" on page 2-32. 2. If the connection test fails, ensure that the repository is live and online. 3. If repository is live and online, ensure that the repository details on the Configuration Manager System Configuration tab are complete and accurate. See "Adding Repository Details in the Configuration Manager" on page 2-29
21	SQL Exception Occurred, While setting Connection's AutoCommit Property To False	1. The repository is down or offline. 2. Repository details on the Configuration Manager System Configuration tab might be inaccurate or incomplete.	Perform the following steps, as needed: 1. Test the repository connection from the System Configuration tab. See "Ensuring the Repository is Available to the Configuration Manager" on page 2-32. 2. If the connection test fails, ensure that the repository is live and online. 3. If repository is live and online, ensure that the repository details on the Configuration Manager System Configuration tab are complete and accurate. See "Adding Repository Details in the Configuration Manager" on page 2-29

Table B–7 (Cont.) Configuration Manager Message, Cause, and Resolution

Number	Message	Cause	Resolution
22	SQL Exception Occurred, While Checking for schema in the database	1. The repository is down or offline. 2. Repository details on the Configuration Manager System Configuration tab might be inaccurate or incomplete.	Perform the following steps, as needed: 1. Test the repository connection from the System Configuration tab. See "Ensuring the Repository is Available to the Configuration Manager" on page 2-32. 2. If the connection test fails, ensure that the repository is live and online. 3. If repository is live and online, ensure that the repository details on the Configuration Manager System Configuration tab are complete and accurate. See "Adding Repository Details in the Configuration Manager" on page 2-29
23	SQL Exception Occurred, While retrieving Environment From Database	1. The repository is down or offline. 2. Repository details on the Configuration Manager System Configuration tab might be inaccurate or incomplete.	Perform the following steps, as needed: 1. Test the repository connection from the System Configuration tab. See "Ensuring the Repository is Available to the Configuration Manager" on page 2-32. 2. If the connection test fails, ensure that the repository is live and online. 3. If repository is live and online, ensure that the repository details on the Configuration Manager System Configuration tab are complete and accurate. See "Adding Repository Details in the Configuration Manager" on page 2-29
24	SQL Exception Occurred, While retrieving Environment Parameters From Database	1. The repository is down or offline. 2. Repository details on the Configuration Manager System Configuration tab might be inaccurate or incomplete.	Perform the following steps, as needed: 1. Test the repository connection from the System Configuration tab. See "Ensuring the Repository is Available to the Configuration Manager" on page 2-32. 2. If the connection test fails, ensure that the repository is live and online. 3. If repository is live and online, ensure that the repository details on the Configuration Manager System Configuration tab are complete and accurate. See "Adding Repository Details in the Configuration Manager" on page 2-29
25	Entry Already Exist in the Database.	The entry you are adding into the repository already exits. For example, the environment or association name exists in the repository.	Enter an unique value.
26	SQLException While Connection Rollback	The repository is down or offline.	Perform the following steps, as needed: 1. Test the repository connection from the System Configuration tab. See "Ensuring the Repository is Available to the Configuration Manager" on page 2-32. 2. If the connection test fails, ensure that repository is live and online.

Table B–7 (Cont.) Configuration Manager Message, Cause, and Resolution

Number	Message	Cause	Resolution
27	Connection failure. For details refer to log file.	LDAP directory environment might not be running or details about this environment in the Configuration Manager might be incomplete or inaccurate.	Perform the following steps, as needed: 1. Click the Test Environment button on the View Environment page to ensure that the directory is live and online. See "Testing the Environment Connection" on page 3-12. 2. Ensure that the LDAP directory environment details are complete and accurate. See "Adding and Managing Environment Details in the Configuration Manager" on page 3-4
28	Error while reading from LDAP Server. For details refer to log file.	LDAP directory environment might not be running or details about this environment in the Configuration Manager might be incomplete or inaccurate.	Perform the following steps, as needed: 1. Click the Test Environment button on the View Environment page to ensure that the directory is live and online. See "Testing the Environment Connection" on page 3-12. 2. Ensure that the LDAP directory environment details are complete and accurate. See "Adding and Managing Environment Details in the Configuration Manager" on page 3-4
29	LdapConnectionException Caught, while getting LDAPDeltaUpdater	LDAP directory environment might not be running or details about this environment in the Configuration Manager might be incomplete or inaccurate.	Perform the following steps, as needed: 1. Click the Test Environment button on the View Environment page to ensure that the directory is live and online. See "Testing the Environment Connection" on page 3-12. 2. Ensure that the LDAP directory environment details are complete and accurate. See "Adding and Managing Environment Details in the Configuration Manager" on page 3-4
30	NamingException Occurred While Performing Delete Operation On Directory	LDAP directory environment might not be running or the node to be deleted might not exist.	Perform the following steps, as needed: 1. Click the Test Environment button on the View Environment page to ensure that the directory is live and online. See "Testing the Environment Connection" on page 3-12. 2. Ensure that the LDAP directory environment details are complete and accurate. See "Adding and Managing Environment Details in the Configuration Manager" on page 3-4
31	Selected environment type differs from actual environment type.	You might have selected the wrong environment type (the parameter that designates the Oracle Access Manager or COREid release).	On the Add Environment or Modify Environment page, select the correct **Environment Type** for this LDAP directory (OAM1014, for example).

Troubleshooting OC4J Installation and Setup Issues

Topics in this section provide tips to help if you encounter problems during OC4J installation and setup, including:

- Changing the Password for the OC4J Administrator
- Configuring OC4J to Recognize Oracle Access Manager Configuration Manager
- Confirming the OC4J Host is Ready for OC4J installation
- Defining Administrator Privileges in OC4J

- Installing OC4J in a Standalone Configuration
- OC4J Welcome Page Fails to Appear
- Starting and Stopping OC4J
- Using the Oracle Enterprise Manager 10g Application Server Control Console

For more information, see troubleshooting tips in the *Oracle Containers for J2EE Configuration and Administration Guide* 10*g* Release (10.1.3).

Changing the Password for the OC4J Administrator

Problem: Changing the Password for the OC4J administrator

During installation you are asked to provide a password for the `oc4jadmin` account. If you do not assign a password for this account when OC4J is installed, you are prompted to set it the first time you start OC4J.

Solution:

For information about changing the password after installation, see the chapter on Tools for Administering OC4J in the *Oracle Containers for J2EE Configuration and Administration Guide* 10*g* Release (10.1.3).

Configuring OC4J to Recognize Oracle Access Manager Configuration Manager

Problem: Configuring OC4J to recognize Oracle Access Manager Configuration Manager

How do I configure OC4J to recognize the Configuration Manager application?

Solution:

You must deploy Oracle Access Manager Configuration Manager using Oc4J, as described in "Deploying the Configuration Manager" on page 2-12. For instructions on creating additional Web sites in OC4J, see the chapter on Managing Web Sites in OC4J in *Oracle Containers for J2EE Configuration and Administration Guide* 10*g* Release (10.1.3).

Confirming the OC4J Host is Ready for OC4J installation

Problem: Confirming the OC4J host is ready for OC4J installation

How can I confirm that the intended host computer is setup appropriately before I install a standalone OC4J server?

Solution:

Before installing a standalone OC4J server, ensure the prerequisites described in "Installing and Configuring OC4J" on page 2-7 are met. For more information, see Chapter 2 of the *Oracle Containers for J2EE Configuration and Administration Guide* 10*g* Release (10.1.3).

Defining Administrator Privileges in OC4J

Problem: Defining administrator privileges in OC4J

How do I define administrator privileges for OC4J?

Solution:

During OC4J standalone installation, you are asked to provide a password for the `oc4jadmin` account. This account is assigned the `oc4j-administrators` role that is used to manage users and roles and to connect to the JMX MBean server. If you do not assign a password for this account when OC4J is installed, you are prompted to set it the first time you start OC4J.

For an overview and steps, "Installing and Configuring OC4J" on page 2-7. For more information about defining administrator privileges in OC4J, see the *Oracle Containers for J2EE Configuration and Administration Guide* 10*g* Release (10.1.3).

Installing OC4J in a Standalone Configuration

Problem: Installing OC4J in a standalone configuration

How do I install OC4J in a standalone configuration to operate with Oracle Access Manager Configuration Manager?

Solution:

The OC4J standalone configuration in installed in the same manner whether you will use it with Oracle Access Manager Configuration Manager or not. For an overview and steps, see "Installing and Configuring OC4J" on page 2-7. For more information, see the chapter on Installing Standalone OC4J in *Oracle Containers for J2EE Configuration and Administration Guide* 10*g* Release (10.1.3).

OC4J Welcome Page Fails to Appear

Problem: OC4J Welcome page fails to appear

After installation, what do I do if the Welcome page does not appear?

Solution:

Confirm that you have entered the appropriate URL for the host, port, and console (`http://hostname:port/em/console`, for example). For specific troubleshooting tips, see the *Oracle Containers for J2EE Configuration and Administration Guide* 10*g* Release (10.1.3).

Starting and Stopping OC4J

Problem: Starting and Stopping OC4J

How do I start and stop OC4J?

Solution:

For information about starting and stopping OC4j, see the corresponding chapter in the *Oracle Containers for J2EE Configuration and Administration Guide* 10*g* Release (10.1.3).

Using the Oracle Enterprise Manager 10*g* Application Server Control Console

Problem: Using the Oracle Enterprise Manager 10*g* Application Server Control Console

Solution:

The Oracle Enterprise Manager 10*g* Application Server Control Console is a Web-based administration application that is installed by default with OC4J and enabled immediately after installation. For more information on using this management interface, see the section on the Oracle Enterprise Manager 10g Application Server Control Console in *Oracle Containers for J2EE Configuration and Administration Guide* 10*g* Release (10.1.3).

Troubleshooting Oracle Database Installation and Setup Issues

This section includes information to assist if you encounter problems or errors installing or setting up the Oracle Database repository for Oracle Access Manager Configuration Manager. The following topics are included:

Installing Oracle Database on a Specific Platform

Problem: Installing on a specific platform

How can I ensure that I have properly set up the intended host before installation?

Solution:

Refer to the appropriate *Oracle Database Server Installation Guide* for your specific platform for installation and setup details.

Oracle Database Administration and Management Issues

Problem: Oracle Database administration and management issues

How can I properly perform administration and management of the Oracle Database?

Solution:

See the *Oracle Database Concepts 10g Release 2 (10.2)* for more information about Oracle Database administration and management.

Managing Oracle Database Processes and File Issues

Problem: Managing Oracle Database processes and files

How can I manage Oracle Database processes and files?

Solution:

Use the *Oracle Database Administrator's Guide 10g Release 2 (10.2)* for details about managing Oracle Database processes, tablespaces, datafiles, tempfiles, managing schema files, Oracle-managed files, and more.

Specifying the Database Service Name

Problem: Oracle Access Manager Configuration Manager reports "SQLException - While creating database connection."

If Oracle Access Manager Configuration Manager does not recognize the service name of the database when it tries to connect, an error is returned: "SQLException - While creating database connection."

Cause:

To connect to the Oracle Database repository, Oracle Access Manager Configuration Manager requires the Database Service Name. You must enter this information in the System Configuration details when adding the repository..

Solution:

You must enter the Database Service Name on the Edit System Configuration page when adding the repository.

Troubleshooting Configuration Manager Issues

If an operation cannot be completed successfully using the Configuration Manager, an error message usually appears to inform you of the problem. Following topics provide information to assist if you encounter problems or errors using Oracle Access Manager Configuration Manager. Topics include:

- Cannot Create a Snapshot
- Cannot Connect to the Database
- Cannot View the Content of an Environment (Directory) Snapshot
- Configuration Manager Installation, Setup, and Repository Issues
- Environment Issues within the Configuration Manager
- Association and Transformation Rule Issues

Cannot Connect to the Database

Problem: SQLException - While creating database connection.

If Oracle Access Manager Configuration Manager does not recognize the service name of the database when it tries to connect, an error is returned: "SQLException - While creating database connection."

Cause:

To connect to the Oracle Database repository, Oracle Access Manager Configuration Manager requires the Database Service Name. Today, however, there is no place to enter this information using the graphical user interface.

Solution:

Edit the DB.Oracle.ServiceName parameter in the Oracle Access Manager Configuration Manager WEB-INF/config/db.properties file, as described in the following procedure.

Cannot Create a Snapshot

Problem: Error occurs and message states "Unable to create snapshot"

Creating a new snapshot operation fails.

Solution:

Test the connection to the environment to ensure that it is live and online, as described in "Testing the Environment Connection" on page 3-12. Test the repository connection to ensure that it is live and online, as described in "Ensuring the Repository is Available to the Configuration Manager" on page 2-32.

Cannot View the Content of an Environment (Directory) Snapshot

Problem: Cannot view the content of an environment (directory) snapshot

During a view snapshot operation, only the snapshot name, description, data created, and individual who created the snapshot are listed.

Solution:

You can view the details about a snapshot; however, you cannot view the contents of a snapshot.

Configuration Manager Installation, Setup, and Repository Issues

Problem: Configuration Manager Welcome page does not appear

The Welcome page does not appear after deploying Oracle Access Manager Configuration Manager.

Solution:

Confirm that you have completed all steps in "Deploying the Configuration Manager" on page 2-12. For more information, see troubleshooting tips related to deploying an application in the *Oracle Containers for J2EE Configuration and Administration Guide*.

Problem: Cannot access the System Configuration tab or add repository details

System Configuration tab not available to add a repository, upload the Configuration Manager schema, or to test the connection between the Configuration Manager and its repository.

Solution:

Oracle Access Manager Configuration Manager System Configuration functions are available only to individuals who log in with `HMAdmin` privileges. For more information, see "Assigning Configuration Manager Administrator and User Roles in OC4J" on page 2-16.

Problem: Schema upload not successful

Not all the database objects were properly uploaded.

Solution:

Confirm that you have the appropriate system privileges to create a table, create a sequence, create a trigger, and create a procedure.

Problem: Repository connection test not successful

When the repository connection test is not successful an error message appears.

Solution:

Confirm that all repository details are accurately entered and edit them if needed. Confirm that the Oracle Database instance is running, then test the connection again as described in "Adding Repository Details in the Configuration Manager" on page 2-29. If the connection test is still unsuccessful, contact the Oracle Database administrator.

Environment Issues within the Configuration Manager

This topic includes solutions to several issues that you can encounter when working with LDAP directory environments in Oracle Access Manager Configuration Manager. Any environment that is involved when making a directory snapshot, migrating data, or rolling back a transaction *must* be live and online.

Problem: Certificate Upload Not Successful

An error message appears when you add environment (directory) details and have an unsuccessful attempt to upload a certificate for SSL-enabled communication.

Solution:

Review the message, then click the Cancel button on the error window. Verify the location of the certificate files and the password, then perform the certificate steps again as described in "Adding Environment Details to the Configuration Manager" on page 3-5.

Problem: Connection Failure

When I test the connection to an environment, the informational message states "Connection failure. For details refer to log file."

Solution:

Notify the directory administrator, and give the location of the log file as described in "Accessing and Using the Log File" on page B-1.

Problem: Environment details not available in Configuration Manager

The environment I want is not listed when I view environments or attempt to form an association.

Solution:

Ensure that the environment (directory) details have been added to the Configuration Manager, as described in "Adding Environment Details to the Configuration Manager" on page 3-5.

Association and Transformation Rule Issues

Problem: Association details not available in Configuration Manager

The association I want is not listed when I view associations or attempt to add a transformation rule.

Solution:

Ensure that the association has been formed, as described in "Creating a Directory Association" on page 3-15.

Association is not listed for selection during migration

The desired association does not appear in the Select Association list on the Migrate subtab, Select Logical Objects to Compare page.

Solution:

Confirm that the desired association is enabled, as described in "Enabling or Disabling a Directory Association" on page 3-16.

Problem: Transformation rule does not operate as expected

After previewing the logical objects to be migrated, it appears that a transformation rule did produce the expected results.

Solution:

View (and modify, if needed) the rule to ensure that it specifies the appropriate logical object type and attribute, as well as the correct operator and parameter. for more information, see "Modifying a Transformation Rule" on page 3-35.

Glossary

association

A term used to describe a designated source directory and target directory pair. Each directory association includes a designated source directory from which logical objects are selected for migration to a designated target directory. All the history related to the migration of logical objects between the designated source and target directory pair belongs to the association.

attribute

One or more characteristics or traits related to logical (and physical) objects. For example, the logical object "Workflow Definition" includes a name attribute and a description attribute in addition to other attributes.

configuration data

Oracle Access Manager, or Oracle COREid, product-specific configuration data and access policy data stored in a Lightweight Directory Access Protocol (LDAP) directory. This data includes workflow and configuration information that governs the appearance and functionality of the Identity System and Access System. Configuration data is managed by the Identity System.

configuration management

Life-cycle management of specific Oracle Access Manager (or Oracle COREid) configuration data. Oracle Access Manager Configuration Manager enables you to push changes from one deployment to another deployment within the same release. See also **environment**.

configuration dn

The bind DN for Oracle Access Manager (or Oracle COREid) configuration data. See also **COREid**

COREid

The product formerly known as "Oblix NetPoint" or "Oblix COREid" has been renamed "Oracle COREid". Oracle COREid Release 7.0.4 was made available as part of Oracle Application Server 10*g* Release 2 (10.1.2). See also **Oracle Access Manager**.

delta

The difference between the logical objects of the source directory and the logical objects of the target directory in an associated pair (prior to migration). See also **logical object**

deployment

Each individual installation of Oracle Access Manager 10*g* (10.1.4.0.1), or Oracle COREid Release 7.0.4, is known as a deployment. Your enterprise can include one or more deployment types, for example a development or QA or production or preproduction deployment. You can have multiple deployments of the same type.

directory

An LDAP directory that is installed and configured for Oracle Access Manager 10*g* (10.1.4.0.1) or Oracle COREid Release 7.0.4. Each directory that you add to Oracle Access Manager Configuration Manager can be designated as either the source or target in an association pair. See also **environment**.

environment

A supported LDAP directory server that is installed and configured to work with Oracle Access Manager 10*g* (10.1.4.0.1), or Oracle COREid Release 7.0.4, within various deployments (development, or QA, or production) within your enterprise. Such directories include either , or Oracle COREid, configuration data stored as physical entities, which correspond to logical objects. See also **logical object**.

export

In the context of Oracle Access Manager Configuration Manager, the term *export* refers to writing configuration data that you select to an LDIF file, which you can use with an external tool to import data to an LDAP directory. See also **import** and**LDIF file**.

horizontal data migration

The process of copying configuration data changes from one Oracle Access Manager 10*g* (10.1.4.0.1), or Oracle COREid Release 7.0.4, deployment to another. You cannot migrate 10*g* (10.1.4.0.1) data to a release 7.0.4 deployment, nor vice versa. See also **environment**.

import

In the context of Oracle Access Manager Configuration Manager, the term *import* refers to opening a file and extracting information in a usable format. For example, after exporting configuration data to an LDIF file using Oracle Access Manager Configuration Manager, you can import data from the LDIF file into an LDAP directory using an external tool. See also **LDIF file**.

LDAP

A Lightweight Directory Access Protocol (LDAP) directory. Data stored in this type of directory is referred to as LDAP data.

LDIF file

Lightweight Directory Interchange Format (LDIF) file. LDIF files are ASCII format files that you can use to exchange and synchronize data between Lightweight Directory Access Protocol (LDAP) servers using an external tool.

logical object

For most applications you can have a repository (a database or directory server) that stores the data as physical entities (tables in a database or LDAP entries in a directory server). Many times, a group of physical entities are logically related so tightly that an individual physical entity cannot make much sense with respect to the application. These physical entities can be grouped together under the name of one object (called a logical object). A logical object can also be a one-to-one mapping with a physical entity.

A logical object can have dependencies on other logical objects. For example in Oracle Access Manager 10*g* (10.1.4.0.1) and Oracle COREid Release 7.0.4, Workflow Definition is configuration information that can be considered as a logical object with dependencies on workflow steps which in turn have dependencies on workflow participants.

Oracle Access Manager Configuration Manager migrates (copies) logical objects from one installed deployment to another. For example, from an Oracle Access Manager 10*g* (10.1.4.0.1) Development directory to another Oracle Access Manager 10*g* (10.1.4.0.1) Development directory or to an Oracle Access Manager 10*g* (10.1.4.0.1) Production directory. Migration of each logical object is atomic (the logical object and all its dependents are copied to the target). See also **LogicalObject**.

LogicalObject

The inmemory structure of the logical object and its attribute-values and the dependent logical objects. This represents the actual logical object that exists in the particular environment (directory). LogicalObject defines the mapping of a logical object type to one or more physical entities. It also defines the dependencies among the logical objects of a directory in an association pair. Migration of one logical object is atomic (the logical object and all its dependents are copied to the target). See also **logical object**.

migration

The process of pushing (copying) selected logical objects (and related physical entities) from the designated source to the designated target directory of an associated pair. For example, if you have defined and tested a new password policy in your QA deployment you can propagate the policy to a Production system using Oracle Access Manager Configuration Manager. When you migrate data, all selected entries in the configuration tree are copied from the source directory server to the target directory server in the associated pair.

`oblix` tree

The directory tree in which Oracle Access Manager, or Oracle COREid Release 7.0.4, configuration and access policy data are stored.

Oracle Access Manager

Starting with release 10*g* (10.1.4.0.1), the product formerly known as Oracle COREid is now named Oracle Access Manager. See also **COREid**.

repository

The datastore that you install for use with Oracle Access Manager Configuration Manager. The repository is where migration information is stored, including migration transaction data, snapshots, LDIF files to import, and audit details. Configuration Manager log files are not stored in the repository.

restore

Restore a directory snapshot to revert changes made to the logical objects since the snapshot.

roll back

Revert changes made during a specific migration transaction and return the logical objects in the target directory to their state before the specific migration. See also **transaction**.

source

The directory in an associated pair in Oracle Access Manager Configuration Manager that is designated to send a copy of the configuration data changes to the target. See also **target**.

snapshot

A backup copy of the configuration data for all logical objects in the designated directory made at a given point in time using Oracle Access Manager Configuration Manager. A snapshot will include only the logical objects (workflow definitions, for example, but not the workflow instances). A snapshot can be used to restore (return) the directory to the state it was in at the time the snapshot was made.

system configuration

A tab in Oracle Access Manager Configuration Manager that enables individuals with the HMAdmin privilege to enter and edit Oracle Access Manager Configuration Manager repository information. See also **repository**.

target

The recipient environment in an Oracle Access Manager Configuration Manager associated pair (the directory designated to receive a copy of the configuration data changes from the source). See also **environment** and **source**.

transaction

Every configuration data migration that is performed using Oracle Access Manager Configuration Manager is referrred to as a transaction. A transaction ID is assigned automatically just before the migration occurs. You can provide an optional transaction description. See also **transaction record**.

transaction record

A record is created each time you migrate configuration data using Oracle Access Manager Configuration Manager. Each transaction record includes the entire group of logical objects (and their dependencies) that were migrated from the source to the target of the associated pair. A list of all transaction records is available. You can choose a particular record and view the changes made during that transaction. You can select a transaction and rollback the changes to restore the target to the state it was in before that migration. See also **transaction**.

transformation rule

A rule you can define for a directory association. A transformation rule enables you to change the value of selected logical object attributes automatically during migration. See also **migration**.

Index

Symbols

Numerics

A

B

C

D

E

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X