Oracle® Fusion Middleware

Transitioning to Oracle Unified Directory

11*g* Release 2 (11.1.2)

E55596-01

April 2015

Documentation that describes how to transition Directory Server Enterprise Edition (DSEE) and Oracle Directory Server Enterprise Edition (ODSEE) deployments to Oracle Unified Directory (OUD).

ORACLE

Oracle Fusion Middleware Transitioning to Oracle Unified Directory, 11*g* Release 2 (11.1.2)

E55596-01

Primary Author: Francisco Franklin

Contributing Authors: Sylvain Duloutre, John Spencer

Contributors: Etienne Remillon, Don Biasotti, Eric Locatelli, Jeanine Pikus

Contents

4 Executing the Transition

Preface

The *Oracle Fusion Middleware Transitioning to Oracle Unified Directory* describes how to transition Sun Directory Server Enterprise Edition and Oracle Directory Server Enterprise Edition to the current release of Oracle Unified Directory. The guide also provides information about transitioning ODSEE Directory Proxy Server instances to OUD proxy instances.

This Preface includes the following sections:

Audience

This guide is intended for directory service administrators who are transitioning to Oracle Unified Directory. The guide might also be useful to business planners who are considering transitioning to Oracle Unified Directory.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at
http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit
http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit
http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Related Documents

For more information, see the following documents in the Oracle Unified Directory 11*g* Release 2 (11.1.2.3) documentation set.

- *Release Notes for Oracle Unified Directory*
- *Administering Oracle Unified Directory*
- *Developing Oracle Unified Directory*

- *Installing Oracle Unified Directory*

Conventions

The following text conventions are used in this guide:

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

Understanding the Transition to Oracle Unified Directory

The transition process to Oracle Unified Directory enables you to replace an existing installation of Directory Server Enterprise Edition with the current release of Oracle Unified Directory.

This chapter includes the following sections:

1.1 Supported Transition Paths

You can transition to Oracle Unified Directory 11*g* Release 2 (11.1.2.3) from:

- Oracle Directory Server Enterprise Edition (ODSEE) 11*g*
- Sun Directory Server Enterprise Edition (DSEE) 7.0
- Sun Java System Enterprise Edition (DSEE) 6.x
- Sun ONE Directory Server / Sun Java System Directory Server (DSEE) 5.2

> **Note:** "(O)DSEE refers to both DSEE and ODSEE directories. ODSEE and DSEE are used in this guide only when the information is specific to that particular directory.

ODSEE, formerly SUN Directory Server Enterprise Edition (DSEE), is the best known directory server with proven large deployments in carrier and enterprise environments.

OUD is an all-in-one directory solution with storage, proxy, synchronization and virtualization capabilities.

OUD provides all the services required for high-performance enterprise and carrier-grade environments. It ensures:

- Scalability to billions of entries
- Ease of installation

- Elastic deployments
- Enterprise manageability
- Effective monitoring
- Excellent performances
- Maximum choice of hardware and operating systems
- Strong adherence to the latest LDAP standards
- Integration with Oracle Fusion Middleware products

OUD and (O)DSEE are part of the same Oracle Directory Services Plus license scheme, however the code base and architecture of the two products differ, so transition to OUD requires some steps that need to be carefully considered.

1.2 Using This Transition Guide

This guide provides upgrading instructions for Directory Server and Directory Proxy Server to Oracle Unified Directory. This guide helps (O)DSEE customers select the best transition strategy based on their system requirements and constraints. After you chose a strategy, step-by-step procedures are provided to transition to OUD and deploy it.

This guide focuses on typical upgrades and it covers the most common use cases. Unique deployments might require additional steps and may be conducted with the help of Oracle Consulting Services.

The approach proposed in this guide consists of taking advantage of new OUD services while preserving your user data and key server configuration so that the transition is transparent for client applications.

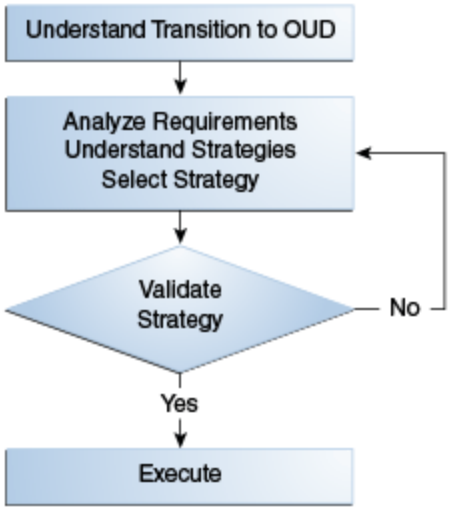
Transition can be a good opportunity to revisit parts of the directory architecture and it can be conducted as part of the transition process, however, improving the infrastructure is not the primary focus of this guide.

1.3 Transitioning to OUD

The following is an overview of the process for transitioning to OUD:

1. Select the best transition strategy after you identify your key requirements related to the transition.
2. Validate the chosen transition strategy based on in-depth diagnosis of the existing (O)DSEE deployment.
3. Execute the validated strategy by performing the steps in this guide.

Figure 1–1 Transitioning Process to OUD



1.4 Transitioning to OUD Proxy

Directory Proxy Server (DPS) is another key element of a complete modern directory service. OUD, when configured as a proxy component, offers the same level of proxy and distribution functionality as the DPS component of DSEE.

As part of your transition plan, you should plan to transition your proxy instances as well. Since both DPS and OUD configured in proxy mode are void of data, this transition mainly consists of migrating the configuration and switching your traffic once your new instances are ready to operate.

Refer to the *Administering Oracle Unified Directory Guide, Section A.2.2* for information on using the `dps2oud` command to transition your DPS instances configuration to OUD.

1.5 Transitioning Synchronization Services

Appendix A, "Transitioning Synchronization Services" of this guide describes how to transition an existing deployment of Identity Synchronization for Windows to Oracle Directory Integration Platform.

For more information about this transition, continue with Appendix A, "Transitioning Synchronization Services."

2

Choosing a Transition Strategy

This chapter provides a methodology to select a transition strategy to transition an existing installation of Directory Server Enterprise Edition to Oracle Unified Directory. Be aware that the selection of the strategy can be an iterative process.

This chapter includes the following sections:

2.1 Analyze Your Requirements

The transition process must be aligned with your architectural and operational requirements. The selection of the right transition strategy is a key factor for a smooth transition to OUD. The following are important factors to consider when selecting a transition strategy:

2.1.1 Coexistence of the (O)DSEE and OUD topologies in production

Using a coexisting approach provides an incremental transition process where the (O)DSEE and OUD deployments coexist and are kept in sync in a production environment while client applications are redirected progressively to OUD. This approach also allows applications to revert back to (O)DSEE without any interruption of service.

It is important to be aware that some added-value services/features provided by OUD cannot be deployed until the end of the coexistence so it is recommended to use this strategy for a specific period of time only. Similarly, the topology will not be able to deliver improved write performance made possible by OUD until changes are no longer replicated back to (O)DSEE.

Keeping two environments in production requires additional system resources because the two infrastructures must be managed separately. Furthermore, keeping the two environments in sync also adds complexity to the system so it is recommended to evaluate whether coexistence is a key requirement or not for your transition project.

2.1.2 Coexistence and data consistency between (O)DSEE and OUD

During replication all data is copied and is in sync and kept up-to-date across servers. However, each server does not necessarily contain identical data, especially metadata. If you choose to have ODSEE and OUD topologies coexist in production, then follow these guidelines:

- Evaluate the level of data consistency you expect between the two environments.
- Decide if you require strong consistency with global replication conflict management to ensure that every change is applied in a coherent and ordered manner.
- Determine how you prefer to handle temporary data consistency by choosing to accommodate synchronization latency or to require near real time data consistency between (O)DSEE and OUD topologies.
- Establish if you require full synchronization of password policy-related state, ensuring consistent account locking across the entire typology.

Note: Projects that require coexistence for a very short period of time may not require fully-featured global password policy support. A conflict may occur when the same entry is modified simultaneously on different servers. In this specific situation, full conflict management guarantees that the entry will be identical on both servers.

2.1.3 Impact of the Transition on the (O)DSEE Infrastructure

In some specific cases, limited changes to the (O)DSEE infrastructure may greatly simplify the transition process and make support of specific features possible. For example, such modifications to (O)DSEE may include addition of LDAP schema extensions, modification of password policy mode or deployment of retro changelog.

Determine whether or not well-identified changes to (ODSEE) are acceptable as part of your transition strategy selection.

2.1.4 Transition With or Without Write Service Interruption

The ability to redirect client traffic from (O)DSEE to OUD without interruption of service is an important factor to consider. Administrators should be aware of the built-in automatic mechanisms that ensure write service during transition. For other projects, the interruption of updates is unacceptable.

Some transition strategies proposed in this guide provide full-write high-availability during transition. Other transition strategies would require deployment of additional components such as proxies able to duplicate traffic.

2.1.5 User Data Structure Change

Before transitioning the directory service, you may want to take the opportunity to evaluate the existing directory services architecture and user data structure. Or, you might be fine with the existing architecture, but want to revisit only a subset of the user data.

This guide does not address transitions that involve redesigning the user data structure. Contact your Oracle Support representative if your transition requires changes to the user data structure.

2.2 Supported Transition Strategies

This section describes the strategies that Oracle supports for your transition, and a decision matrix to assist you in choosing the transition strategy that best fits your technological needs. Choose one of the following strategies:

- Section 2.2.1, "Coexistence Using the Replication Gateway"

- Section 2.2.2, "Coexistence Using Oracle Directory Integration Platform (DIP)"
- Section 2.2.3, "Direct Transition Strategy"

2.2.1 Coexistence Using the Replication Gateway

With this strategy, (O)DSEE and OUD topologies are kept in sync at the native replication protocol level by using the Replication Gateway. Replication through the Gateway has very low latency because it does not involve any polling mechanism.

The Replication Gateway is installed and managed like any other OUD component and performs the required adaptation of replication protocols between (O)DSEE and OUD. The Replication Gateway provides strong data consistency between the two types of directories and fully leverages conflict management. As full directory metadata are replicated, the Replication Gateway also synchronizes internal password policy states, ensuring proper account locking.

The Replication Gateway offers a true two-way replication between (O)DSEE and OUD. It is a high-performance conduit that propagates the updates between heterogeneous replicated topologies without being stored at the gateway level. A unit of replication is the suffix as defined on the (O)DSEE side. You can also run the Replication Gateway in one-way mode so that changes from your directory server are replicated to OUD while changes from OUD will not be reflected on (O)DSEE.

For high availability, at least two Replication Gateway servers are deployed between two (O)DSEE masters and two OUD replication servers in every scenario. This eliminates the risk of a single point of failure.

2.2.2 Coexistence Using Oracle Directory Integration Platform (DIP)

Oracle Directory Integration Platform (DIP) is a multi-purpose synchronization tool used among various repositories and it enables you to do the following:

- Synchronize (O)DSEE and OUD topologies.
- Run your directory server with OUD as you transition over time with no downtime.
- Use the changelogs configured on (O)DSEE and OUD to detect changes and replay them back and forth.

Synchronization triggers periodically and processes a configurable maximum number of changes at each run. DIP synchronizes user data only.

For more information about DIP, refer to the *Oracle Directory Integration Platform (DIP) Administrator's Guide*. You can access that document in the Oracle Fusion Middleware 11*g* Release 1 (11.1.1.7) library located at
http://www.oracle.com/technetwork/middleware/id-mgmt/documentation/index.html

2.2.3 Direct Transition Strategy

This strategy uses export and import methods with standard directory administrative commands. The user data and configuration are exported from (O)DSEE, and adapted if necessary, using tools and procedures described in this guide. The user data and configuration are then imported into OUD.

The Direct Transition Strategy is a singular transition, and it is simple and quick. It can be used when interruptions on write capabilities are acceptable. Directory Administrators typically use a load balancer or an LDAP proxy to put the

infrastructure in read-only mode, export data from (O)DSEE, import the data to OUD, then redirect the traffic to OUD.

2.2.4 Decision Matrix

The following decision matrix summarizes the key decisions factors in choosing a transition strategy:

Table 2–1 Decision Factors for Transition Strategies

Decision Factors	Coexistence Using Replication Gateway	Coexistence Using DIP	Direct Transition
Coexistence	Yes	Yes	No
Data Consistency Level	Strong Low Latency	Loose Latency Depends on DIP Configuration	N/A
Performance	High	Medium	N/A
Impact on (O)DSEE	Depends on (O)DSEE release and setting (Chapter 3, "Validating Your Transition Strategy")	Enable retro changelog	No
Write service availability	Built-in support	Built-in support	Requires additional components (*)
Data adaptation/ Structure changes	No	Yes (limitations apply)	Yes (can be performed at will)
High Availability	Built-in Support	Deployment Specific	N/A

(*) not covered in this guide

3

Validating Your Transition Strategy

After choosing a strategy to transition Directory Server Enterprise Edition to Oracle Unified Directory, the next step is to validate your strategy. This chapter provides guidance for uncovering potential roadblocks and for validating your strategy choice.

This chapter includes the following sections:

3.1 Validate the Selected Strategy

To validate that you have selected the best transition strategy, you should consider all of these aspects for your chosen strategy: (O)DSEE release, password policy version used, and whether (O)DSEE-specific features like Roles and Class of Services are used in addition to what was identified in Chapter 2, "Choosing a Transition Strategy."

3.2 Considering DSEE Versions

The DSEE version impacts transition when replication gateway is used in the following ways:

- Password Policy State Replication

  DSEE 5.2 uses a set of password policy attributes. Starting with DSEE 6.0, a new set of standard password policy attributes (DS6-mode) was introduced. The choice between DSEE 5.2 password policy and DS6 password policy is made by configuration.

  OUD and the Replication Gateway manage standard attributes. Fully-functional password policy between (O)DSEE and OUD requires every (O)DSEE instance to run in DS6-mode.

  The switch from default password policy mode to DS6-mode requires administrative action.

  For information on password policy see the "Password Policy Compatibility" section of the *Administrator's Guide for Oracle Directory Server Enterprise Edition*. That document can be found in the Oracle Directory Server Enterprise Edition 11*g* Release 1 (11.1.1.7) library located at
  `http://www.oracle.com/technetwork/middleware/id-mgmt/documentation/index.html`

DSEE 5.2 instances or any (O)DSEE instance with old password policy mode in the existing (O)DSEE topology, requires schema extension on both (O)DSEE and OUD.

- Replication Gateway Integration

  The Replication Gateway must communicate with one compatible ODSEE master instance. This means that the ODSEE server connected to the Replication Gateway needs to be at least an ODSEE 11gR1 (11.1.1.5) instance. If none is available, a ODSEE 11g must be added to the topology for use by the Replication Gateway. You can keep this ODSEE 11gR1 and its Replication Gateway located on the same box, or you can upgrade any existing instance to at least ODSEE11gR1 (11.1.1.5.)

Note: With OUD 11gR2 (11.1.2.3) the replication gateway can communicate with a DSEE 6.3 instance, while older versions, such as DSEE 5.2, still require the addition of an ODSEE 11g instance.

Figure 3–1 Transition process to OUD using the Replication Gateway

3.3 Adapting (O)DSEE Legacy Features

The following must be adapted for OUD use regardless of the strategy chosen:

- Role-based ACIs
- Roles and Class of Services (CoS)
- Custom Password Policies

3.3.1 Role-based ACIs

Role-based ACIs can be used to manage access to data, based on user role. Role-based ACIs are not supported by OUD 11*g* R2 Release 2 (11.1.2.3), so such ACIs must be adapted and replaced by group-based ACIs during the transition process, regardless of the strategy in use.

With the Replication Gateway Strategy, every directory metadata are replicated, including ACIs. This means that role-based ACIs must be replaced by group-based ACIs on (O)DSEE before putting coexistence in place.

When the DIP Strategy is used, you need to either adapt such ACIs on (O)DSEE before deploying synchronization, or consider excluding synchronization of such ACIs.

For more information on Role-based ACIs see the *Administrator's Guide for Oracle Directory Server Enterprise Edition*. That document can be found in the Oracle Directory Server Enterprise Edition 11*g* Release 1 (11.1.1.7) library located at `http://www.oracle.com/technetwork/middleware/id-mgmt/documentation/index.html`

3.3.2 Roles and Class of Services (CoS)

(O)DSEE Roles and Class of Services must be replaced to equivalent OUD mechanisms as described in section Section 4.6.6, "Transitioning Roles to OUD," and Section 4.6.5, "Managing Class of Service (CoS)." In some cases, the corresponding OUD mechanism requires the use of directory metadata. For example, Class of Service definitions can be replaced by OUD Collective Attributes definitions stored along with user data.

When the Replication Gateway Strategy is used, these OUD-specific metadata may be replicated back to (O)DSEE. In such cases, (O)DSEE schema must be extended to support these additional attributes and objectclasses. An extract of the OUD schema that can be used on (O)DSEE servers for compatibility reasons is available with OUD: `INSTALL_DIR/config/ds2oud/99OudSchemaExtract.ldif`

For more information on Roles and CoS see the *Administrator's Guide for Oracle Directory Server Enterprise Edition*. That document can be found in the Oracle Directory Server Enterprise Edition 11*g* Release 1 (11.1.1.7) library located at http://www.oracle.com/technetwork/middleware/id-mgmt/documentation/index.html

3.3.3 Custom Password Policies

Custom password policies can be stored as part of the data in (O)DSEE. Such password policy definitions are made of standard attributes (supported by OUD) and (O)DSEE-specific attributes (replaced by other attributes in OUD). Furthermore, assignment of a password policy to a given user entry differs between (O)DSEE and OUD.

With the Replication Gateway Strategy, some OUD-specific metadata may be replicated back, requiring (O)DSEE schema extensions. An extract of the OUD schema that can be used on ODSEE servers for compatibility reasons is available with OUD: `INSTALL_DIR/config/ds2oud/99OudSchemaExtract.ldif`

For more information on Custom Password Policies see the *Administrator's Guide for Oracle Directory Server Enterprise Edition*. That document can be found in the Oracle Directory Server Enterprise Edition 11*g* Release 1 (11.1.1.7) library located at http://www.oracle.com/technetwork/middleware/id-mgmt/documentation/index.html

3.3.4 Managing Data Inconsistencies

Characteristics of user data stored in (O)DSEE may impact transition because OUD implements full schema check, including attribute value syntax validation. (O)DSEE does not implement full schema check so, some values accepted on the (O)DSEE side might be rejected by OUD. These data inconsistencies can be identified using diagnostic tools that ship with OUD. These issues may be addressed in several ways, including fixing the data before transition, fixing the schema, or making some checks on OUD, flexible.

3.4 Review: Impact of Technical (O)DSEE Characteristics

In the following tables, the impact of technical (O)DSEE characteristics are summarized. Also, note that an asterisk (*) indicates the preferred option if your transition does not require two-way replication. Using this option reduces the impact on the (O)DSEE side since one-way replication only replicates changes from (O)DSEE to OUD.

Table 3–1 Existing Directory Server Release

Directory Server Release	Replication Gateway	DIP	Direct
DSEE 5.2	■ Deploy one ODSEE 11*g* instance as a gateway companion. ■ Extend DSEE schema with OUD password policy (*). ■ Limitation: password policies on (O)DSEE and OUD are decoupled	■ Limitation: password policies on (O)DSEE and OUD are decoupled	■ Limitation: password policy state is reset during transition.
DSEE 6.x/7.x	■ Extend DSEE schema with OUD password policy (*). ■ Upgrade DSEE password policy mode if needed.	■ Limitation: password policies on (O)DSEE and OUD are decoupled.	■ Limitation: password policy state is reset during transition.
ODSEE 11gR1+	■ Extend DSEE schema with OUD password policy if no global password policy needed & stick to old password policy mode (*). ■ Upgrade DSEE password policy mode if needed.	■ Limitation: password policies on (O)DSEE and OUD are decoupled.	■ Limitation: password policy state is reset during transition.

Table 3–2 Existing Directory Server Data

Existing Directory Server Data	Replication Gateway	DIP	Direct
Metadata: Role-based ACIs	■ Update DSEE ACIs before transition.	■ Update DSEE ACIs before transition or ■ Adapt ACIs on OUD & don't synchronize ACIs.	■ Adapt ACIs.
Metadata: CoS/Roles	■ Adapt CoS/Roles. ■ Optionally, extend DSEE schema (*).	■ Adapt CoS/Roles (not synchronized).	■ Adapt CoS/Roles.
Metadata: Password policies as sub entry (in the data)	■ Adapt password policies. ■ Optionally, update password policies before transition.	■ Custom password policies not synchronized or adapted if possible.	■ Adapt password policies.

Table 3–2 (Cont.) Existing Directory Server Data

Existing Directory Server Data	Replication Gateway	DIP	Direct
Invalid data in DSEE (do not fully match LDAP schema).	▪ Fix data in DSEE or ▪ Relax schema checks on OUD or ▪ Update schema on OUD.	▪ Fix data in DSEE or ▪ Relax schema checks on OUD or ▪ Update schema on OUD.	▪ Fix data in DSEE or ▪ Relax schema checks on OUD or ▪ Update schema on OUD.

3.4.1 Using ds2oud to Identify Relevant (O)DSEE Features

OUD provides `ds2oud`, a diagnostic tool that automatically identifies (O)DSEE features that impact your transition. In diagnostic mode, `ds2oud` can also identify (O)DSEE-specific features currently in use which do not have an exact counterpart on OUD. This includes Roles and Class of Services. The `ds2oud` tool is useful for every strategy as it transitions configuration and schema, and identifies (O)DSEE features that must be adapted. The `ds2oud` tool is especially useful when the Replication Gateway strategy is used because the gateway replicates directory metadata in addition to user data. This tool also analyses (O)DSEE schema and data to make sure they conform to the LDAP schema as implemented by OUD.

For more information about running the `ds2oud` command in diagnostic mode, see *Section A.2.3, "ds2oud," in the Administering Oracle Unified Directory Guide.*

The *Administering Oracle Unified Directory Guide,* can be found at `http://www.oracle.com/technetwork/middleware/id-mgmt/documentation/index.html`

4

Executing the Transition

This chapter describes the steps you must perform to transition Directory Server Enterprise Edition to Oracle Unified Directory.

This chapter includes the following sections:

4.1 Starting Your Transition to OUD

This chapter explains the steps you must perform to transition to OUD. You must perform all steps in this chapter regardless of which transition strategy you are using.

Note: If you are using the Direct Strategy, then skip to: Section 4.7, "Step 6: Deploying Replication Gateway or DIP."

4.2 Step 1: Creating a Reference OUD Instance

You must first install OUD 11g Release 2 (11.1.2) and create a new instance. The new OUD instance is configured and initialized during the transition steps, and then used as a base to configure and deploy additional instances in a replicated topology.

For instructions on installing an OUD instance, see *Installing Oracle Unified Directory*.

You can set up a new OUD instance using one of the following methods:

- Graphical User Interface (GUI)
- Command Line Interface (CLI)

- Batch mode

In order for the `ds2oud` command to work successfully, you must configure the new instance with no suffixes.

To set up your directory server by using the GUI or by using the CLI, the suffix/base `dn` must be left blank. Refer to the *Installing Oracle Unified Directory Guide* for setting up the directory server using the GUI and CLI.

When the directory server is set up in batch mode, the `-b` options must not be specified.

Note: The `ds2oud` command is located in `<OUD_INSTANCE>/OUD/bin`. `OUD_INSTANCE` is the path of the base OUD instance created in Section 4.2, "Step 1: Creating a Reference OUD Instance."

4.3 Step 2: Using ds2oud to Diagnose the (O)DSEE Directory Server, Configuration, Schema and Data

During this step, existing (O)DSEE settings are analyzed to identify the features that do not have an identical counterpart on the OUD side and cannot be transitioned automatically. These features will require special attention during transition.

Ensure that you have the LDAP administrative password to access the (O)DSEE directory server. No changes will be performed on this server during the diagnostic cycle. For further information, see *Understanding Root Users and the Privilege Subsystem in the Administering Oracle Unified Directory Guide.*

Ensure that you have an LDIF file containing the user data exported from your (O)DSEE directory server. For information on exporting LDIF files, go to the following:

- For information on exporting LDIF files for 5.2, refer to the "Exporting Databases" section in the *Sun ONE Directory Server 5.2 Reference Manual*. You can access the Reference Manual on the Sun Java Enterprise System 2003Q4 web site located at `http://docs.oracle.com/cd/E19199-01/`
- For information on exporting LDIF files for 6.x, refer to the "Exporting to LDIF" section in the *Sun Java System Directory Server Enterprise Edition 6.3 Administration Guide.* You can access the Administration Guide in the Sun Java System Directory Server Enterprise Edition 6.3 web site located at `http://docs.oracle.com/cd/E19261-01/`
- For information on exporting LDIF files for 7.0, refer to the "Exporting to LDIF" section in the *Sun Directory Server Enterprise Edition 7.0 Administration Guide*. You can access the Administration Guide in the Sun Directory Server Enterprise Edition 7.0 web site located at `http://docs.oracle.com/cd/E19424-01/`
- For information on exporting LDIF files for 11*g*, refer to the "Exporting to LDIF" section in the *Oracle Directory Server Enterprise Edition Administration Guide*. You can access the Administration Guide in the Oracle Directory Server Enterprise Edition 11*g* Release 1 (11.1.1.5) library located at `http://www.oracle.com/technetwork/middleware/id-mgmt/documentation/index.html`

Ensure that you have access to a copy of the user schema extensions `(99user.ldif)` holding the (O)DSEE server schema extension.

This diagnostic process is performed by running the `ds2oud` tool which is shipped with OUD. The number of differences detected by `ds2oud` in diagnostic mode can be used to estimate complexity and transition effort.

4.3.1 Diagnose the (O)DSEE Directory Server, Configuration and Schema

Run the following `ds2oud` command to diagnose your server configuration that must be transitioned to OUD:

```
$ ds2oud --diagnose -h host1.example.com -p 1389 \
  -D "cn=directory manager" -j pwdfile
```

In the command above, host1 is the (O)DSEE server, not the OUD server.

The --diagnose subcommand identifies the following elements of your directory server configuration:

- Unsupported plug-ins
- Extensions to the default schema
- The type of password policy used which may have an impact if you use the Replication Gateway Strategy
- Encrypted attributes
- Index settings
- Global configuration parameters

For each element above, `ds2oud` identifies what needs to transition and potential incompatibilities (if any). Below is an *example* of an output:

```
*** diagnose the deployment ...


********************************************************************************
Diagnose ODSEE Server : host1:1389
********************************************************************************


** Plugins : No user plugins are defined, nothing particular to migrate

** Plugins : No subtree counter plugins are enabled, nothing particular to
migrate

** Schema

The schema was extended regarding the original delivery. The following schema
should be added to the new OUD server
attributeTypes : ( 2.16.840.1.113730.9999 NAME 'customAttributeType' DESC
'Oracle defined attribute type' SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
SINGLE-VALUE X-ORIGIN ( 'Custom' 'user defined' ) )

** Password Policy

A compatible password policy is defined, nothing particular to migrate

** Naming context(s) available on the ODSEE server :
o=migration


No incompatibility has been detected for naming context o=migration
```

```
** Indexes

Only default indexes are defined, nothing particular to migrate

** Encrypted attributes
No encrypted attributes are defined, no action is required
```

4.3.2 Diagnose the Directory Server Data

To verify that your directory server data is compliant with OUD schema before importing the data:

1. Export the data to LDIF from your directory server. For information on exporting data to LDIF, see Section 4.2, "Step 1: Creating a Reference OUD Instance."
2. Run the `ds2oud` command to diagnose the data. For example:

   ```
   $ ds2oud --ldifDBFile odsee-data.ldif --userSchemaFile 99user.ldif
   ```

   In this example `odsee-data.ldif` is your directory server data exported to LDIF and `99user.ldif` is your customized directory server schema file. Below is an example of output during data diagnostic:

   ```
   *** diagnose the data ...


   ********************************************************************************
   * Diagnose ODSEE LDIF data file :
   odsee-data.ldif
   ********************************************************************************

   Error validating data against OUD schema
   Entry : unknown
   org.opends.sdk.DecodeException: Entry uid=user2,ou=users,o=data read from LDIF
   starting at line 49 includes value "" for attribute description that is invalid
   according to the associated syntax: The operation attempted to assign a
   zero-length value to an attribute with the directory string syntax
   ```

4.3.3 Known Errors During Diagnosing

Schema errors may be reported for the following reasons:

- Default schema is different.
- OUD has a more recent version of standard schema.
- Attribute value syntax validation and containment rules validations.
- Unsupported directory metadata. This includes role-based ACIs, Roles or Class of Services definitions currently not supported by OUD password policies as LDAP sub-entries. These sub-entries contain (O)DSEE specific extensions account-based resource limits that differ between (O)DSEE and OUD.

In the above cases, OUD provides the commands below to make schema constraints flexible and resolve those schema errors.

Structural `objectclass` errors:

Structural `objectclass` errors occur when your directory server data is rejected during an import. A common reason for this error is the structural object-class for the user entry. The user entry must have exactly one structural object-class. If the entry has zero

or more than one, the entry will be rejected. Also, because your (O)DSEE directory server does not differentiate between the two object-class types, this kind of schema inconsistency is common. Use the following command to avoid this error:

```
dsconfig set-global-configuration-prop --set \
single-structural-objectclass-behavior:accept -n
```

Invalid attribute value errors:

Attribute values must conform to the attribute syntax defined in the schema. By default, attribute syntax checking is enabled in OUD. For example, an attribute with Boolean syntax can hold TRUE or FALSE values only. In addition, zero-length attribute values are rejected by OUD during an import. However it is possible to make this constraints flexible for the DirectoryString syntax by using this command:

```
dsconfig set-attribute-syntax-prop --syntax-name Directory\ String \
--set allow-zero-length-values:true -n
```

4.4 Step 3: Transitioning Directory Schema

When you transition the directory user schema, the (O)DSEE schema extensions are automatically added to the OUD reference instance schema using the `ds2oud` tool in migration mode.

Schema is migrated automatically using the `ds2oud` tool. You must migrate the schema before you migrate the configuration or errors will be triggered during subsequent transition steps. The following command propagates the user schema from your (O)DSEE directory server to OUD and it can also be used to migrate the (O)DSEE schema to other OUD instances:

```
$ ds2oud --migrateUserSchema -h host1.example.com -p 1389 \
  -D "cn=directory manager" -j pwdfile
```

To migrate the (O)DSEE schema to other OUD instances, you can also copy the content of the `<OUD_INSTANCE>/OUD/config/schema` directory to the corresponding directory of the new OUD instance, then restart the OUD instance.

Note: Although the `ds2oud --migrateUserSchema` command handles any extensions made on the (O)DSEE user schema, schema violations still may occur when you import your user data into OUD. This happens because, unlike user-defined schema, standard schema varies slightly between (O)DSEE and OUD. If schema violations occur during the import process, then you must create additional schema extensions which are likely suggested as a result of the (O)DSEE diagnosis process.

4.5 Step 4: Transitioning Directory Configuration

During this step, the OUD reference instance is configured so that it can provide an LDAP service equivalent to (O)DSEE.

Most of the (O)DSEE directory configuration is migrated automatically using the `ds2oud` tool in migration mode. Additional configuration elements that cannot be migrated automatically have been identified in Section 4.3, "Step 2: Using ds2oud to Diagnose the (O)DSEE Directory Server, Configuration, Schema and Data."

Configuration commands generated automatically are kept in a batch file so that they can be reused to initialize other instances quickly. Oracle recommends that additional commands created manually, should also be added to that batch file.

4.5.1 Using the ds2oud Command to Migrate the Configuration Settings

Run the `ds2oud` command to migrate the following configuration settings from your (O)DSEE directory server to OUD:

- Naming contexts
- Global configuration settings that are relevant for OUD
- Size-limit
- Look-through-limit
- Idle-time-limit
- Max-psearches
- Bind-with-dn-require-password
- Allidthresholds
- Database indexes
- Global default access controls
- Supported built-in plug-ins
- 7-bit check
- UID uniqueness plug-in
- Referential integrity plug-in
- Strong password policy check

To apply each of the above configuration settings to each OUD instance, you must run the `ds2oud` command in batch mode. It will then generate a list of commands to be applied with `dsconfig`. This is recommended to be able to complement changes and replay them easily on every target system.

To produce the administrative command batch file to transition the configuration, run the following command:

```
ds2oud --migrateConfiguration
       --odseeBindDN "cn=directory manager"
       --odseePort <ODSEE_PORT>
       --odseeBindPasswordFile <ODSEE_ADMIN_PASSWORD_FILE>
       --oudBindDN "cn=directory manager"
       --oudBindPasswordFile <OUD_ADMIN_PASSWORD_FILE1>
       --oudPort <OUD_LDAP_PORT1>
       --oudAdminPort <OUD_ADMIN_PORT1>
       --no-prompt --batchFile <COMMAND_BATCH_FILE>
```

4.5.1.1 Migrating SSL Certificates

By default, self-signed certificates are automatically generated when OUD instances are created. In some cases you might want to reuse the (O)DSEE server certificate for the new OUD instance, so that the transition is transparent for SSL clients. This, however, might require installation of the OUD instance on the same box as the (O)DSEE server depending on SSL certificate options used.

To reuse the SSL server certificate, do the following:

1. Export the directory server certificate to a PKCS12 file. In the following example, `dsee.p12` is the PKCS12 filename.

   ```
   dsadm export-cert -o dsee.p12  <instance_path> defaultCert
   ```

   Note: By default, the alias of the directory server cert is defaultCert. Use the appropriate alias in case you choose to use another value. You can find more information on exporting a directory server in the *Administering Oracle Unified Directory Guide*.

2. Copy the PKCS12 file to `<OUD_INSTANCE>/config`.
3. Create a PIN file containing the PKCS12 file password such as `dsee.p12.pin` in the `<OUD_INSTANCE>/config` directory. The directory server certificate can be imported in the OUD instance in two different ways:
   - Configure a PKCS12 OUD keystore pointing to the file exported from your directory server.
   - Import the certificate to the default JKS OUD keystore.

4.5.1.2 Configuring the PKCS#12 Keystore

To configure the OUD PKCS12 keystore run the following command:

```
dsconfig set-key-manager-provider-prop \
         -provider-name PKCS12 \
         -set key-store-file:config/dsee.p12 \
         -set key-store-pin-file:config/dsee.p12.pin \
         -set enabled:true \
```

In these code samples, when we use the `dsconfig` command connectivity-related arguments such as ports and credentials are omitted for the sake of simplicity.

4.5.1.3 Configuring the LDAPS Connection Handler to use the PKCS#12 keystore

To configure the LDAPS connection run the following command:

```
dsconfig set-connection-handler-prop \
         --handler-name LDAPS\ Connection\ Handler \
         --set key-manager-provider:PKCS12 \
```

4.5.1.4 Importing the Directory Server Certificate Key Pair

To import the certificate to the existing OUD JKS keystore, do the following:

1. Locate the JAVA_HOME of the JVM used by OUD. The version of the JVM used is displayed at startup in the OUD error log.
2. Run the following command to import the certificate:

   ```
   JAVA_HOME/bin/keytool -v -importkeystore -srckeystore <Path to PKCS12 cert file
   exported from DSEE>  -srcstoretype PKCS12 -destkeystore <OUD_INSTANCE_
   DIR>/OUD/config/keystore  -deststoretype JKS
   ```

   When prompted, specify the JKS PIN (available in `<OUD_INSTANCE_DIR>/OUD/config/keystore.pin`) and the PKCS12 PIN you used to export the DSEE server certificate.

3. Verify that the import operation was successful.

   To list the content of the OUD JKS keystore, use the following:

   ```
   JAVA_HOME/bin/keytool -list -keystore <OUD_INSTANCE_DIR>/OUD/config/keystore
   ```

   Enter keystore password:

   Keystore type: JKS

   Keystore provider: SUN

   Your keystore contains two entries:

   ```
   defaultcert, Aug 29, 2013, PrivateKeyEntry, Certificate fingerprint (MD5):
   10:63:DC:B5:6B:C8:F3:A0:6B:A7:23:9E:0B:EA:9C:30
   server-cert, Aug 29, 2013, PrivateKeyEntry, Certificate fingerprint (MD5):
   BE:C9:F3:8A:49:98:96:15:EF:AC:B4:08:6F:76:FB:05
   ```

   By default, the (O)DSEE directory server certificate alias is "`defaultCert`", the OUD server certificate alias is "`server-cert`" and Java automatically chooses the best certificate among those present in the keystore. If you want to force the use of one certificate, run this command:

   ```
   dsconfig set-connection-handler-prop \
   --handler-name LDAPS\ Connection\ Handler \
   --set ssl-cert-nickname:defaultcert \
   ```

4.5.1.5 Migrating Encrypted Attributes

Use `--decrypt-attr` option with `dsconf export` to decrypt attributes.You must make sure that attributes are decrypted when exported to the LDIF file. Corresponding attribute encryption must be configured in OUD so that values are re-encrypted during import.

You can find instructions to configure encrypted attributes in OUD in the *Administering Oracle Unified Directory Guide*.

4.5.2 Changing Password Storage Scheme for Coexistence

You must change the OUD password storage scheme configuration if you are using either coexistence strategy, that is, Replication Gateway or DIP. This will ensure that the password storage scheme configured on the OUD side corresponds to an algorithm supported by (O)DSEE. Otherwise, users will not be able to log in anymore on the (O)DSEE side when the password is modified on the OUD side. In (O)DSEE, passwords are stored using some password encryption scheme, such as, `SHA-1`. In OUD, this is similar but passwords are stored by default in `SSHA512`.

In OUD, password storage scheme is configured in password policies.

4.5.3 Applying Configuration Changes

Configuration changes generated in Section 4.5.1, "Using the ds2oud Command to Migrate the Configuration Settings," can be applied to the OUD directory server instance with the following command:

```
dsconfig -h <oud hostname> -p <oud admin port> -D cn="directory manager" -w <admin
password> \
  -F command_batch_file -X -n
```

The `-F` or `--batchFilePath` option of the `dsconfig` command enables you to specify a number of operations that are completed in a single command by consolidating those operations in a file. This can significantly improve performance and simplify configuration of other instances when several `dsconfig` commands are required.

Additional configuration changes identified in Section 4.5.1.1, "Migrating SSL Certificates," need to be applied also.

Note: Schema changes must always be applied before configuration changes. These configuration changes will have to be applied on each OUD instance deployed later. For more information see, Section 4.7.1, "Deploying The Replication Gateway,"

4.6 Step 5: Transitioning User Data and Directory Metadata

Once the OUD reference instance is configured, it is loaded with actual (O)DSEE user data and directory metadata.

4.6.1 Exporting User Data from (O)DSEE to OUD

User data present in your directory server must first be exported to the LDIF format so that they can be reimported to OUD. Go to Section 4.3, "Step 2: Using ds2oud to Diagnose the (O)DSEE Directory Server, Configuration, Schema and Data," for information on exporting to LDIF files.

The data to be exported depends on the chosen transition strategy. For example, if you are using the Direct Transition Strategy or the Transition Strategy Using DIP, replication metadata that accounts for a large volume of the data on the disk should be filtered out at export time. But for the Transition Strategy using Replication Gateway, replication metadata is needed.

If you are using the Direct Transition Strategy or the Transition Strategy Using DIP, run the `dsconf` export command as shown in the following example to export the user data to LDIF:

```
$ dsconf export --no-repl --decrypt-attr \
-h host1.example.com -p 1389 \
dc=example,dc=com odsee-data.ldif
```

If you are using Transition Using Replication Gateway Strategy the replication metadata must be kept and adapted to OUD format. To export the user data to LDIF using this strategy, run the `dsconf export` command as shown in the following example:

```
$ dsconf export -f opends-export --decrypt-attr -h host1.example.com -p 1389 \
  dc=example,dc=com odsee-data.ldif
```

Note: The option `-f opends-export` in the preceding command is only applicable for ODSEE 11*g* Release 1 (11.1.1.5 or later) since the data must be exported from the ODSEE 11*g* master which is required if you are using the Replication Gateway. Also note that encrypted data on the disk must be decrypted during export.

To produce an LDIF file for DSEE 6.3 (DSEE 6.3 does not provide the -f option):

1. Export the LDIF from DSEE 6.3 using `dsconf` command (do not include -f)
2. Run `ds2oud --adaptDseeData` <path to LDIF file> (This generates a new LDIF file <path to LDIF file>_result.ldif)
3. Import the generated file into OUD by using the command: `import-ldif -b <your user data suffix> -n <db name e.g userRoot> --excludeAttribute "nsds5replconflict" -l <path to LDIF file_ result.ldif>`

4.6.2 Importing Data to OUD

The `import-ldif` command is used to populate an OUD directory server backend with data read from an LDIF file. The following is an `import-ldif` example:

```
import-ldif -b <your user data suffix>  -n userRoot --excludeAttribute
"nsds5replconflict"  -l <path to LDIF file>
```

When you use the `opends-export` option during transition, (O)DSEE-specific attributes might exist in some entries which will prevent these entries from being imported. For instance, `nds5replconflict` might exist in the (O)DSEE data so it is imperative to filter this attribute during import to OUD using the following import option:

```
--excludeAttribute "nsds5replconflict"
```

4.6.3 Transitioning Directory Metadata

Directory metadata transition depends on the transition strategy you have chosen to use. This may include access control information (ACI), collective attributes and LDAP sub entries.

- For the Direct Transition Strategy: the directory metadata only needs to be adapted once.
- For the Replication Gateway Strategy: directory metadata are replicated between the directory server and OUD. The directory metadata must be kept compatible on both sides. However, some metadata are different between the two environments, so additional schema extensions will be required to avoid errors or loss of data.
- For the DIP Strategy: DIP should be configured to synchronize user data. The directory metadata is generally added manually on OUD. In some cases, DIP can be configured to synchronize the metadata.

Access to data is managed with access control instructions (ACIs) that specify the access rights of entries. ACIs can be stored as part of the user data or in the OUD configuration.

- **Global ACIs vs. ACIs in the data**

Global ACIs apply to all entries in the directory. They are stored in the configuration. (O)DSEE and OUD global ACIs can differ without causing errors as they are not replicated.

The `ds2oud` tool migrates the global ACIs to OUD global ACIs automatically.

ACIs that are stored as part of the data, are replicated.

- **Differences with Syntax**

  The `roledn` keyword is currently not supported in OUD 11*g* Release 2. ACIs with the `roledn` keyword cannot be imported into OUD because ACI syntax checking fails. Roles can be replaced by groups and the `roledn` keyword can be replaced by `groupdn` (See Roles and ACIs).

  A new value for the `targetscope` keyword, `subordinate`, is introduced in OUD. This value is not supported by (O)DSEE so it must not be used in a two-way replication topology between (O)DSEE and OUD.

- **Behavioral Differences**

  In a few cases, evaluation of the same ACI differs between (O)DSEE and OUD. Since OUD grants less access by default than (O)DSEE, you will need to grant additional write access during the transition so that OUD behaves like (O)DSEE. In such cases, OUD ACI evaluation would be more inflexible than on the (O)DSEE side.

  By default, OUD ACIs don't allow users to reset another user's password. With OUD, a privilege must be added to achieve behavior that is equivalent to that of (O)DSEE. Alternatively, it is possible to disable the privilege subsystem. For example, the command below allows the admin to reset user passwords in (O)DSEE (this type of password reset is refused by default in OUD):

```
ldapmodify -p <dsee port> -D "cn=directory manager"-w <admin password
dn: dc=example,dc=com
changetype: modify
replace: aci
aci: (targetattr = "*") (version 3.0;acl "Custom LDAP Administrator";allow
(all)(userdn = "ldap:///uid=admin,dc=example,dc=com");)
```

  With OUD, the following privilege below must be added to achieve the equivalent behavior:

```
dn: uid=admin,dc=example,dc=com
changetype: modify
add: ds-privilege-name
ds-privilege-name: password-reset
```

  Alternatively, the privilege subsystem can be disabled using the following command:

```
dsconfig set-global-configuration-prop  -add disabled-privilege:password-reset
```

4.6.4 Managing ACIs in Replication Topologies

When (O)DSEE and OUD do not need to coexist in a replication topology, ACIs can be manually adapted, if needed, before importing them into OUD, as described previously.

When one-way replication is used, ACIs present in the data on (O)DSEE may have to be adapted manually before transition. Invalid ACIs will not be imported during

replication initialization because of ACI syntax checking. ACIs updates on the (O)DSEE side might still be replicated to OUD but they will not be applied on the OUD side.

If you have incompatible ACIs, an alternate is to configure the Replication Gateway to filter out ACIs during replication. Each (O)DSEE ACI would be filtered out and the administrator would need to create the corresponding ACIs in OUD, either as part of the data or in the configuration.

For two-way replication between (O)DSEE and OUD, the same recommendations as for one-way replication applies. In addition, OUD-specific ACIs extensions must not be used in a mixed environment.

Note: (O)DSEE and OUD ACIs are compatible except, in some cases, when (O)DSEE specific keywords as `roleDN` are used.

4.6.5 Managing Class of Service (CoS)

Class of Services definitions are stored as LDAP sub entries along with the user data.

Class of Services functionality is currently not supported in OUD. When replication is configured between (O)DSEE and OUD, CoS definitions are automatically filtered out by the Replication Gateway.

CoS can be replaced by the standard Collective Attributes mechanism or by Virtual Attributes. In a replicated topology, computed attributes are generated by CoS on the (O)DSEE side while the equivalent computation is achieved with Collective Attributes or Virtual attribute on the OUD side.

4.6.5.1 Collective vs. Virtual Attributes

Collective attributes definitions are stored as LDAP sub entries along with the user data, which means that they are replicated. Collective attributes provide fine-grained scoping control through the generic sub-entry subtree specifications. Virtual attributes are stored in the OUD configuration and are not subject to replication.

When two-way replication is enabled between (O)DSEE and OUD, you should use Virtual Attributes instead of Collective attributes because Collective Attributes definitions are replicated back to (O)DSEE.

If you specifically need to use Collective attributes (see Section 4.6.5.4, "Classic CoS" and Section 4.6.5.3, "Indirect CoS"), the (O)DSEE schema should be extended with the schema object that pertain to Collective Attributes. In this case, the LDAP sub entries will be present in (O)DSEE but they will be inactive. This means that they will not cause any attribute computation.

The schema definition associated with the `collectiveAttributeSubentry` and `subentry` object classes (present in the OUD schema file `00-core.ldif`) and the associated attributes can be added to the (O)DSEE schema.

Note: In (O)DSEE, CoS is often used in conjunction with roles and password policies. For example, they can be used to assign a custom password policy to a set of users. OUD provides new ways to assign password policies to user accounts. Therefore, in many cases, there are simple alternatives to CoS.

(O)DSEE Class Of Service type is covered in detail in the following sections.

4.6.5.2 Pointer CoS

(O)DSEE Pointer CoS can be used to share a common attribute among a set of entries.

The following (O)DSEE Pointer CoS below automatically assigns a `facsimiletelephonenumber` with a fixed value (+61245607890) to all entries located under `ou=People,dc=example,dc=com`.

```
dn: cn=ZipTemplate,ou=People,dc=example,dc=com
objectclass: top
objectclass: LDAPsubentry
objectclass: extensibleobject
objectclass: cosTemplate
facsimiletelephonenumber: +61245607890
cosPriority: 0

dn: cn=pointerCoS,ou=People,dc=example,dc=com
objectclass: top
objectclass: LDAPsubentry
objectclass: cosSuperDefinition
objectclass: cosPointerDefinition
cosTemplateDn: cn=ZipTemplate,ou=People,dc=example,dc=com
cosAttribute: facsimiletelephonenumber
```

The following OUD virtual attribute can be used to compute an equivalent attribute value: this example creates and enables a virtual attribute rule that adds a virtual fax number of +61245607890 to any user entry matching the `objectclass=person` filter (unless there is already a fax number in the user entry):

```
dsconfig -h localhost -p 4444 -D "cn=directory manager" -j <password_file> -n \
create-virtual-attribute \
--type user-defined -name "Sydney Fax Number" \
--set attribute-type:facsimiletelephonenumber -set enabled:true \
--set value:+61245607890 -set filter:"(objectClass=person)"
```

Unlike virtual attributes, collective attributes are stored along with user data, so they are replicated across OUD instances.

The following collective attribute generates a *facsimiletelephonenumber* for entries in the sub-tree `ou=people,dc=example,dc=com`

```
dn: cn=People Preferred Language,dc=example,dc=com
changetype: add
objectClass: top
objectClass: subentry
objectClass: collectiveAttributeSubentry
objectClass: extensibleObject
cn: People fac simile number
facsimiletelephonenumber;collective: +61245607890
subtreeSpecification: {base "ou=people", minimum 1}
collectiveConflictBehavior: virtual-overrides-real
```

4.6.5.3 Indirect CoS

(O)DSEE Indirect CoS names an attribute in the `cosIndirectSpecifier` attribute to locate the template specific to each target. The template entry for indirect CoS can be any entry in the directory, including other user entries. The following indirect CoS example uses the manager attribute of the target entry to identify the CoS template entry. The template entry is the manager's user entry. The manager's user entry contains the value of the attribute to generate. In this case, the value is that of the `departmentNumber` attribute.

```
dn: cn=generateDeptNum,ou=People,dc=example,dc=com
objectclass: top
objectclass: LDAPsubentry
objectclass: cosSuperDefinition
objectclass: cosIndirectDefinition
cosIndirectSpecifier: manager
cosAttribute: departmentNumber

dn: cn=Carla Fuentes,ou=People,dc=example,dc=com
objectclass: cosTemplate
objectclass: person
departmentNumber: 318842
cn: Carla Fuentes
```

Inherited collective attributes can be used to replace Indirect CoS. Like regular collective attributes, inherited collective attributes are defined using LDAP sub-entries within the directory tree where they are applicable. Inherited collective attributes are replicated across OUD instances. If two-way replication is used between (O)DSEE and OUD, the (O)DSEE schema should be extended with the Collective Attribute schema element as described in Section 4.6.5.1, "Collective vs. Virtual Attributes." The following inherited collective attribute is equivalent to the Indirect CoS definition described previously.

```
dn: cn=indirectCOS,dc=example,dc=com
objectClass: top
objectClass: subentry
objectClass: inheritedCollectiveAttributeSubentry
objectClass: inheritedFromDNCollectiveAttributeSubentry
cn: indirectCOS
subtreeSpecification: {base "ou=people"}
inheritFromDNAttribute: manager
inheritAttribute: departmentNumber
```

4.6.5.4 Classic CoS

This example shows how to generate a postal address value with a classic CoS definition. The generated value is specified in a template entry that is located by a combination of the `cosTemplateDN` in the CoS definition and the value of the `cosSpecifier` attribute in the target entry. The following example creates the definition entry by using the `cosClassicDefinition` object class:

```
dn: cn=classicCoS,dc=example,dc=com
objectclass: top
objectclass: LDAPsubentry
objectclass: cosSuperDefinition
objectclass: cosClassicDefinition
cosTemplateDn: ou=templates,ou=People,dc=example,dc=com
cosSpecifier: building
cosAttribute: postalAddress

dn: cn=B07,ou=templates, ou=People,dc=example,dc=com
objectclass: top
objectclass: LDAPsubentry
objectclass: extensibleobject
objectclass: cosTemplate
postalAddres: 7 Old Oak Street, Anytown, CA 95054
```

With this CoS definition, target entries (the entries under `ou=People,dc=example,dc=com`) that contain the `building` attribute will automatically

have the corresponding postal address. The CoS mechanism searches for a template entry that has the specifier attribute value in its RDN. In this example, if Babs Jensen is assigned to building B07, her postal address is generated.

Equivalent behavior can be achieved in OUD with inherited collective attributes as follow:

```
dn: cn=classicCOS,dc=example,dc=com
objectClass: top
objectClass: subentry
objectClass: inheritedCollectiveAttributeSubentry
objectClass: inheritedFromRDNCollectiveAttributeSubentry
cn: classicCOS
subtreeSpecification: {base "ou=people"}
inheritFromBaseRDN: ou=templates
inheritFromRDNAttribute: building
inheritFromRDNType: cn
inheritAttribute: postalAddress
```

This inherited collective attribute sub-entry applies to user entries under `ou=people,dc=example,dc=com`. The subentry adds the postalAddress attribute inherited from the user entry whose DN is constructed from ou=templates, the Inherited collective attribute sub-entry root DN `dc=example,dc=com` and the RDN cn value taken from applicable entry building attribute, if any.

Like regular collective attributes, inherited collective attributes are defined using LDAP sub-entries within the directory tree where they are applicable. They are replicated across OUD instances. If two-way replication is used between (O)DSEE and OUD, the (O)DSEE schema should be extended with the collective attribute schema element as described in the Section 4.6.5.1, "Collective vs. Virtual Attributes."

4.6.6 Transitioning Roles to OUD

Non-standard (O)DSEE roles are currently not supported in OUD 11*g* Release 2 (11.1.2) and are usually replaced by standard OUD groups. Role definitions are filtered out by the Replication Gateway.

The steps required to transition (O)DSEE roles to OUD depend on the way in which the roles are exposed to external client applications. In many deployments, roles are not exposed to client applications, that is, applications do not make use of the `nsRole` or `nsRoleDN` attributes. Such roles can be replaced by either static or dynamic groups for ACIs and password policies.

4.6.6.1 Roles and ACIs

The `roledn` ACI keyword can be used to grant/deny access to data based on user role. For example, the following (O)DSEE ACI grants access to the user password attribute to users with 'Password Manager' role.

```
dn: ou=data,o=example.com
aci: (targetattr="userPassword")(version 3.0; acl "PasswordManager";allow
(read,search,compare,write) roledn = "ldap:///cn=Password_Manager_
Role,ou=roles,dc=example,dc=com";
```

The `roledn` keyword is not supported in OUD 11*g* Release 2 (11.1.2). This has the following implications:

- ACIs with the `roledn` keyword cannot be imported into OUD 11g Release 2 (11.2.2).

- ACIs present in the (O)DSEE data will not be applied to OUD. These ACIs will be replicated to OUD but changes will not be applied because the ACI syntax does not work for OUD

Roles used in ACIs should be replaced by groups using the `groupdn` keyword before transition. For OUD, the preceding ACI above can be rewritten as:

```
dn: ou=data,o=example.com
aci: (targetattr="userPassword")(version 3.0; acl "PasswordManager";allow
(read,search,compare,write) groupdn = "ldap:///cn=Password_Manager_
Group,ou=group,dc=example,dc=com";
```

The group pointed to by the ACI can be either a static group or a dynamic group.

To migrate role-based ACIs to group-based ACIs before you transition to OUD, you must:

- Define groups that correspond to the roles (using the same DN)
- Rewrite ACIs on the (O)DSEE side before transitioning to OUD

> **Note:** Role-based ACIs present in the (O)DSEE configuration are not replicated, so they do not need to be rewritten.

4.6.6.1.1 Roles and Password Policies

In many deployments, roles are used to assign custom password policies based on role membership. For example, users with the Admin role are subject to the Administrator password policy. In this use case, roles are used in conjunction with CoS to create the virtual attribute `pwdPolicySubEntry` in every user entry pointing to the password policy that should be used.

In OUD, a password policy can be associated directly with members of a group by using a virtual attribute. The following example associates the `adminPasswordPolicy` password policy with members of the `administrator` group.

```
dsconfig create-virtual-attribute -name "PWPolicy for Admins"
--type user-defined
--set attribute-type:ds-pwp-password-policy-dn
--set group-dn:cn=administrators,ou=groups,dc=example,dc=com
--set conflict-behavior:real-overrides-virtual
--set value:"cn=adminPasswordPolicy,ou=policies,ddc=example,dc=com"
```

> **Note:** Unlike CoS, the virtual attribute above that associates password policies with roles is not replicated across OUD instances.

4.6.6.1.2 Roles Exposed to Client Applications

If you are using the Direct Transition Strategy or Transition Using DIP Strategy (the following is not compatible with the Transition Using Replication Gateway Strategy), use the `nsRole` attribute in the target user's entry to determine whether the DN of the appropriate role is present when you need to determine whether a user is a member of a given role in an application. In this case, role functionality can be simulated by following steps:

- Extend OUD schema with the `nsRole` attribute definition (this schema is provided in the file `03-dsee-roles.ldif`)

- Create static or dynamic groups to define role membership. You must reuse the role DNs when you create the groups so that the nsRole attribute content is not impacted.
- Create a new instance of the isMemberOf virtual attribute to provide the nsRole virtual attribute as follow:

```
dsconfig -h localhost -p 4444 -D "cn=directory manager" -j <password_file> -n \
create-virtual-attribute -type is-member-of -name nsRole -set \
attribute-type:nsRole -set enabled:true
```

> **Note:** Virtual attribute definitions are stored in the OUD configuration and thus are not replicated. They must be configured on every OUD instance.

If the application alters membership by placing the name of the corresponding role in the nsRoleDN virtual attribute in a user's entry, create a dynamic group for each role (you must reuse the role DN), and extend the group memberURL filter so that it takes into account the nsRoleDN for group membership. In the following example, any user entry that contains a nsRoleDN value of "cn=Test Role,ou=Roles,dc=example,dc=com" also has that DN present in the nsRole operational attribute.

```
dn: cn=Test Role,ou=Roles,dc=example,dc=com
objectClass: top
objectClass: groupOfURLs
cn: Test Role
memberURL: ldap:///dc=example,dc=com??sub?(nsRoleDN=\
  cn=Test Role,ou=Roles,dc=example,dc=com)
```

If your application needs to create, modify or delete role entries (for example, an entry containing one of the subordinates of the nsRoleDefinition object class), that functionality is currently not available in OUD.

4.6.6.1.3 Transitioning Roles Securely

In OUD, roles are replaced by groups. To use the corresponding groups securely, you must set access control instructions (ACIs) to protect appropriate attributes. With dynamic groups, you must protect the part of the filter that would prevent the user from being able to relinquish the filtered group by modifying an attribute. Users should not be allowed to add, delete, or modify the attribute used by the filtered groups. In the same way, if the value of the filter attribute is computed, all the attributes that can modify the value of the filter attribute must be protected.

4.6.7 Managing Password Policies Transition to OUD

The ds2oud tool, provided with OUD, migrates the standard attributes of the default password policy only. See Table 4–1, " Password Extensions for (O)DSEE and OUD" for password policy mapping from (O)DSEE to OUD.

Custom password policies can be stored either in the data or in the OUD configuration and can be assigned to target users by mean of an attribute in the user entry or based on the position of the sub entry in the DIT. Selecting the best options is key for a successful password policy transition. Ease of use and impact on the OUD administration should be considered (for example, password policies as sub-entries are replicated across OUD instances, password policies in the configuration are not). In addition, not all combinations are possible in OUD 11*g* Release 2 (11.1.2)

The following options must be selected based on your deployment constraints:

- Store custom password policies as sub entries or in the OUD configuration
- Use attributes in user entries or use the sub entry sub tree specification to assign password policies
- If an attribute in user entry is used to assign the password policy, use an explicit setting, virtual attributes or collective attributes to populate the attribute
- Reuse or filter out (O)DSEE password policies during replication

The main decision criteria to be considered are:

- Does the (O)DSEE custom password policy rely on specific extensions?
- Is replication used with (O)DSEE one-way only?
- Is the (O)DSEE custom password policy sub-entry position compatible with OUD?
- Is password policy assignment based on group memberships?

The following is a summary of the differences between OUD and (O)DSEE password policies:

- The (O)DSEE password policy definition consists of standard attributes (defined in the `pwdPolicy` object class) and specific extensions (defined in the `sunPwdPolicy` object class)
- OUD password policies also rely on standard attributes (defined in the `pwdPolicy` object class). However, (O)DSEE-specific extensions are currently not supported in OUD 11*g* Release 2: Such extensions are automatically filtered out during replication and must be replaced by OUD-specific extensions defined in the `ds-cfg-password-policy` object class.

Manual Adaptations required to migrate these extensions are summarized in the table below:

Table 4–1 Password Extensions for (O)DSEE and OUD

(O)DSEE Extensions	OUD Extensions
PasswordStorageScheme	default-password-storage-scheme
PwdKeepLastAuthTime	last-login-time-attribute, last-login-time-format
PasswordRootDnMayByPassModsChecks	skip-validation-for-administrators
pwdIsLockoutPrioritized	N/A
PwdCheckQuality	password-validator

In addition to the global password policy, you can create custom password policies. In (O)DSEE, custom password policies are stored as part of the data, as LDAP sub entries.

In OUD, custom password policies can be stored as part of the data, as LDAP sub entries, or directly in the OUD configuration.

In OUD, password policies defined as LDAP sub entries must rely on standard attributes only (see above) and cannot contain any extensions. This restriction does not apply to password policies stored in the OUD configuration.

4.6.7.1 Password Policy Assignments

In (O)DSEE, a password policy is assigned to a user account based on the value of the `pwdPolicySubEntry` attribute. The attribute value can be either stored physically in the user entry or dynamically populated with CoS based on criteria matched by the entry. The location of the password policy LDAP sub entry is not used to assign the policy to target users. The default password policy applies when the `pwdPolicySubEntry` attribute is not present in a user entry.

In OUD, a password policy can be assigned to a user account in two ways:

- By setting the attribute `ds-pwp-password-policy-dn`, either explicitly or via a virtual or collective attribute, as in (O)DSEE
- By creating the password policy sub-entry in the DIT so that all user entries are below the password policy entry and target user entries match the LDAP filter/ subtree specification present in the sub-entry. Sub-entry sub-tree specification is defined in RFC3672.

The following example corresponds to the first case: the password policy `ServiceAccount` is assigned to members of the group `group_FirstLoginPolicy` by creating a virtual attribute that populates the attribute `ds-pwp-password-policy-dn` based on group membership:

```
dn: cn=group_FirstLoginPolicy,dc=example,dc=com
objectClass: groupOfURLs
MemberURL: ldap://ou=people,dc=example,dc=com??sub? (pwdReset=TRUE)
cn:group_FirstLoginPolicy

dsconfig create-virtual-attribute --name "PWPolicy to Admins" \
--type user-defined --set attribute-type:ds-pwp-password-policy-dn \
--set group-dn:cn=group_FirstLoginPolicy,dc=example,dc=com \
--set conflict-behavior:real-overrides-virtual \
--set value:"cn=ServiceAccount,ou=passwordPolicies,ou=config,dc=example,dc=com"
```

The following example corresponds to the second case: the policy `FirstLoginPolicy` applies to users who are members of the group newbees in the subtree `ou=people,dc=example,dc=com`.

```
dn: cn=FirstLoginPolicy,dc=example,dc=com
objectClass: subentry
Objectclass: pwdpolicy
SubtreeSpecification: { specificationFilter "ismemberOf=cn=group_
FirstLoginPolicy,dc=example,dc=com"}
PwdMaxFailure: 2
PwdAttribute: userPassword
cn:FirstLoginPolicy
```

> **Note:** The subtree specification as implemented in OUD is a super-set of the standard: OUD considers any well-formed LDAP filter as a valid value for the `specificationFilter` attribute. This is a very convenient way to assign password policies based on group membership as shown in the preceding example.

4.6.7.2 Password Policy Inheritance

Evaluation of custom password policies differs between (O)DSEE and OUD. In (O)DSEE, a custom password policy overrides the default password policy settings. With OUD, a custom password policy inherits from the default password policy: Properties not defined at the custom policy level are taken from the default password

policy at the functional level (even if the attribute names do not correspond). These differences must be taken into account during transition.

4.6.7.3 Password Policy and Replication Gateway

When OUD and (O)DSEE coexist in a replicated topology, password policies should be kept as consistent as possible between the two environments, even when they are not replicated through the replication protocol. For example, if password validators differ, a password could be valid on one side and considered invalid on the other side, leading to inconsistencies.

If account lockout is enabled for a given set of entries on (O)DSEE and disabled on OUD (or the reverse), a password reset will not unlock the account on the other side.

4.6.7.4 Replication Gateway and Upgrading (O)DSEE Password Policy

In a replicated topology with global password policy and account lockout across the entire topology, the (O)DSEE servers that communicate directly with the Replication Gateway must run with the password policy in `DS6mode` and the user entries must not contain data related to previous password policy mode. (This is not a must have if you don't need global password policy and when OUD and (O)DSEE can have its own password policy management.) Other (O)DSEE servers can run in compatibility mode, but such deployment is not the preferred one.

For more information about changing password policy modes, refer to the *Administrator's Guide for Oracle Directory Enterprise Edition 11g*.

The command `dsconf get-server-prop pwd-compat-mode` can be used to retrieve the current password policy mode.

By default, ODSEE 11*g* Release 2 uses the `DS5-compatible` mode. You must switch to `DS6-mode` before exporting data from (O)DSEE. To switch to `DS6-mode`, you will need to first switch to the intermediate DS6-migration mode.

The process to switch to `DS6-mode` and regenerate user entries is described in the "Password Policy Compatibility" section in the *Administrator's Guide for Oracle Directory Server Enterprise Edition*.You can access that document in the Oracle Fusion Middleware 11*g* Release 1 (11.1.1.7) library located at http://www.oracle.com/technetwork/middleware/id-mgmt/documentation/index.html

4.6.7.5 Account Lockout

Both (O)DSEE and OUD allow you to configure password policies to force the lockout of accounts after a specified number of failed bind attempts. In addition, it is possible to lock an account manually. The locked account remains locked until the account is activated.

Transition of account state (locked/unlocked) between (O)DSEE and OUD require specific settings. In (O)DSEE, manual account lock relies on Roles: Locked entries are assigned `nsRoleDN=cn=nsManagedDisabledRole,dc=com role`. On OUD, manual account lock relies on the boolean attribute `ds-pwp-account-disabled`. To automatically import a manually locked account from (O)DSEE to OUD, use the following steps:

1. Create a collective attribute on OUD to map the `nsroledn:nsRoleDN=cn=nsManagedDisabledRole to ds-pwp-account-disabled: true`

```
ldapmodify -a
dn: cn=ManagedDisabledAttribute,<dc=example>
```

```
objectClass: top
objectClass: subentry
objectClass: collectiveAttributeSubentry
objectClass: extensibleObject
cn: ManagedDisabledAttribute
ds-pwp-account-disabled;collective: true
subtreeSpecification: {specificationFilter
"nsRoleDN=cn=nsManagedDisabledRole,dc=com"}
```

2. Extend the OUD schema with the `nsroledn` operational attribute:

```
ldapmodify
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: ( 2.16.840.1.113730.3.1.575 NAME 'nsRoleDN' DESC 'Sun ONE
defined attribute type' SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 USAGE
directoryOperation X-DS-USE 'internal' X-ORIGIN 'Sun ONE Directory Server' )
```

One-way (O)DSEE->OUD) replication of locked account require changes in the Replication Gateway configuration: By default, the `nsroledn` attribute is not replicated and is filtered out by the Replication Gateway. This filtering rule must be removed by running the following command:

```
dsconfig set-plugin-prop --plugin-name Gateway\ Plugin --remove
dsee-specific-attribute-types:nsroledn
```

Note: the `nsroledn` attribute must not be used by any application on the OUD side. It is replicated to convey account state information only.

Two-way replication of account lockout requires additional settings on OUD.

3. Extend (O)DSEE schema to add the `ds-pwp-account-disabled` operational attribute:

```
ldapmodify
dn: cn=schema
changetype: modify
add: attributeTypes
@ attributeTypes: ( 1.3.6.1.4.1.26027.1.1.166 NAME 'ds-pwp-account-disabled'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.7 SINGLE-VALUE USAGE directoryOperation
X-ORIGIN 'OpenDS Directory Server' )
```

4. Create a filtered role on (O)DSEE to map account lockout from OUD:

```
ldapmodify -a
dn: cn=OUD_DisabledRole,<dc=example>
objectclass: top
objectclass: LDAPsubentry
objectclass: nsRoleDefinition
objectclass: nsComplexRoleDefinition
objectclass: nsFilteredRoleDefinition
cn: OUD_DisabledRole
nsRoleFilter: (ds-pwp-account-disabled=true)
Description: filtered role to map account lockout from OUD
```

5. Integrate the previous filtered role in the nested role used to disable the account on ODSEE:

```
ldapmodify
dn: cn=nsDisabledRole,dc=com
changetype: modify
add: nsRoleDN
nsRoleDN: cn=OUD_DisabledRole,dc=com
```

Note: When an account is locked in (O)DSEE, the state information is replicated to OUD so the account is also locked in OUD. However, account unlock must be performed on both sides ((O)DSEE and OUD)

An account can also be locked explicitly on (O)DSEE using the `nsAccountLock` attribute.The equivalent attribute in OUD is `ds-pwp-account-disabled`. Some client applications might rely on the `nsAccountLock` attribute. In this case, the easiest way to address this is to declare `nsAccountLock` as an attribute alias for `ds-pwp-account-disabled` in the OUD schema as shown below:

```
attributeTypes: ( 1.3.6.1.4.1.26027.1.1.166
 NAME ( 'ds-pwp-account-disabled' 'nsAccountLock' )
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
 SINGLE-VALUE
 USAGE directoryOperation
 X-ORIGIN 'OpenDS Directory Server' )
```

4.6.7.6 Custom Resource Limits

In (O)DSEE, the following limits can be associated with a password policy:

- The look-through limit specifies the maximum number of entries examined for a search operation.
- The size limit specifies the maximum number of entries returned in response to a search operation.
- The time limit specifies the maximum time spent processing a search operation.
- The idle time-out specifies the maximum time a client connection can remain idle before the connection is dropped.

More information on setting account limits refer to the "Setting Resource Limits For Each Client Account" section in the *Oracle Fusion Middleware Administration Guide for Oracle Directory Server Enterprise Edition*. You can find that document in the Oracle Directory Server Enterprise Edition 11*g* Release 1 index page located at http://docs.oracle.com/cd/E19656-01/

In addition to that, these limits can be set for specific account/user entries: Some (O)DSEE entries may contain the following resource limit attributes: `nsSizeLimit, nsTimeLimit, nsLookThroughLimit, nsIdleTimeout`.

Corresponding attributes on OUD are: `ds-rlim-size-limit, ds-rlim-time-limit, ds-rlim-lookthrough-limit,ds-rlim-idle-time-limit`.

Account-based resource limits are not taken into account by `ds2oud` and must be migrated manually.

When the Replication Gateway is used, the OUD schema `(02-config.ldif)` must be modified so that each (O)DSEE attribute name related to resource limits is declared as an alias name for each corresponding OUD attribute.

In (O)DSEE, -1 is used to disable a resource limit. In OUD, 0 is used. One way to address this difference is to create a virtual attribute on OUD to override the content of the OUD attribute when the value of the (O)DSEE attribute is equal to -1. A virtual attribute must be created for the four attributes. Below are descriptions:

```
attributeTypes: ( 1.3.6.1.4.1.26027.1.1.166
 NAME ( 'ds-pwp-account-disabled' 'nsAccountLock' )
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
 SINGLE-VALUE
 USAGE directoryOperation
 X-ORIGIN 'OpenDS Directory Server' )

dsconfig create-virtual-attribute --name "mapping nsTimeLimit " \
--type user-defined --set attribute-type:ds-rlim-time-limit \
--set filter:"(nsTimeLimit=-1)" \
--set conflict-behavior:virtual-overrides-real \
--set value:"0" \
--set enabled:true

dsconfig create-virtual-attribute --name "mapping nsLookthroughLimit " \
--type user-defined --set attribute-type:ds-rlim-lookthrough-limit \
--set filter:"(nsLookthroughLimit=-1)" \
--set conflict-behavior:virtual-overrides-real \
--set value:"0" \
--set enabled:true

dsconfig create-virtual-attribute --name "mapping nsIdleTimeout " \
--type user-defined --set attribute-type:ds-rlim-idle-time-limit \
--set filter:"(nsIdleTimeout=-1)" \
--set conflict-behavior:virtual-overrides-real \
--set value:"0" \
--set enabled:true
```

For the sake of performance, it is recommended to index the four attributes above for 'presence'.

> **Note:** With the settings above, (O)DSEE resource limit attribute names must always be used even on the OUD side. Use of the OUD attribute name cannot be used when (O)DSEE and OUD cohabit in the same replication topology.

4.7 Step 6: Deploying Replication Gateway or DIP

After completing Section 4.6, "Step 5: Transitioning User Data and Directory Metadata," selected applications can be validated against the OUD servers. If you have chosen:

- "Coexistence Using the Replication Gateway," see Section 4.7.1, "Deploying The Replication Gateway," for instructions to deploy the Replication Gateway.
- "Coexistence Using Oracle Directory Integration Platform (DIP)," see Section 4.7.2, "Deploying DIP," for instructions to deploy DIP.
- "Direct Transition Strategy," continue to Step 7: Deploying Replicated Topology.

4.7.1 Deploying The Replication Gateway

Below are additional components to configure the replication between (O)DSEE and OUD using the Replication Gateway.

Install and configure the Replication Gateway, as described in "Setting Up the Replication Gateway" section in *Oracle Fusion Middleware Installing Oracle Unified Directory*.

At this point you must configure a global administrator for replication. If you intend to connect this server to an existing replicated OUD topology at a later stage, use the same global administrator credentials that you have defined on the other OUD servers.

For example, assuming an existing OUD topology, your server layout prior to transition would be as follows:

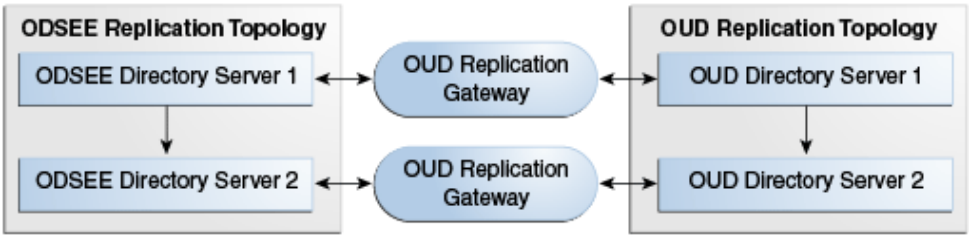
Figure 4–1 Replication Server Topologies for (O)DSEE and OUD Prior to Transition

This figure shows the replication server topologies for ODSEE and OUD before transitioning using the Replication Gateway.

****

After transition, your server layout would be as follows:

Figure 4–2 Replication Server Topologies for (O)DSEE and OUD After Transition



4.7.2 Deploying DIP

Below are additional components to link between (O)DSEE and OUD using DIP. The procedures below configure the (O)DSEE server as the DIP backend directory so that your DIP-related metadata is no longer stored in OUD after you have deprovisioned your old directory server and DIP has been removed.

1. Choose the (O)DSEE master instance and the OUD directory server instance that will be synchronized. The OUD directory server must have an embedded replication server because the external changelog services is provided by replication servers.
2. Synchronize password storage schemes

Password storage schemes must be identical and compatible between (O)DSEE and OUD. To configure password storage schemes to enable synchronization refer to the "Default Password Policy" section in the *Administrator's Guide for Oracle Unified Directory*. You can find that document in the Oracle Unified Directory 11*g* Release 2 (11.1.2) library located at http://www.oracle.com/technetwork/middleware/id-mgmt/documentation/index.html

3. Create a directory suffix holding DIP metadata in (O)DSEE

   Use the following command on DSEE 6.x (or higher) to create the suffix `cn=products,cn=oraclecontext`to hold DIP metadata:

   ```
   dsconf create-suffix -i -c -p $PORT -D "$ADMIN" -w "$PW_FILE"
   cn=products,cn=oraclecontext
   ```

   For instructions for how to create the directory suffix for DSEE 5.2 see the *Sun ONE Directory Server Administration Guide*. That document is located in the Sun Java Enterprise System 2003Q4 index page located at

   http://docs.oracle.com/cd/E19199-01/

4. Enable changelog

   Changelog must be enabled on the directory that will contain changes. Enable changelog on (O)DSEE with the following command:

   ```
   dsconf set-server-prop -p $PORT -w "$PW_FILE" retro-cl-enabled:on
   ```

   For two-way synchronization, external changelog must be enabled on OUD. By default, the external changelog is automatically enabled when the OUD instance is part of a replication topology. For testing purposes, set up a standalone OUD directory server instance and enable external changelog with the following command:

   ```
   dsreplication enable-changelog --no-prompt --baseDN "dc=example,dc=com"
   --hostname "$HOST" --port $APORT --bindDN "$ADMIN" --adminPasswordFile "$PW_
   FILE" --trustAll
   ```

5. Install and configure DIP.

   1. Install DIP in a Weblogic container.

      For more information about on installing DIP in a Weblogic container, refer to the *Oracle Directory Integration Platform Administrator's Guide*. You can access that document in the Oracle Fusion Middleware 11*g* Release 1 (11.1.1.7) library located at http://www.oracle.com/technetwork/middleware/id-mgmt/documentation/index.html

   2. Configure DIP with the command below:

      ```
      $ORACLE_HOME/bin/dipConfigurator setup -wlshost <hostname> -wlsport <admin_
      server_domain_Port> -wlsuser weblogic -ldaphost <dsee_host> -ldapport
      <dsee_port> -ldapuser "dsee_administrator" -metadatasuffix
      cn=products,cn=oraclecontext -isldapssl false
      ```

      The `<dsee_administrator>`, for example, `cn=directory` manager must be granted read and write access to the DIP metadata suffix (`cn=products,cn=oraclecontext`).

In the default password policy, the `allow-pre-encoded` option must be 'true.' This will allow the `<dsee_administrator>` to have access to write pre-encoded password.

For LDAP users, the following command will change the default password policy:

```
dsconfig set-password-policy-prop --policy-name Default\ Password\ Policy
--set allow-pre-encoded-passwords: true
```

SSL users refer to the DIP Administrator's Guide to manage certificates

6. Create synchronization profiles.

   Ensure that the oud_ldap_administrator, e.g. cn=directory manager has read and write access to the suffix to be synchronized. Also, when two-way synchronization is used, it must have read access on the OUD External changelog.

   There are two ways to synchronize profiles: the command line and DIP graphical user interface (EM). The following is an example to synchronize profiles using the command line:

   ```
   $ORACLE_HOME/bin/expressSyncSetup -h <dip_hostname> -p <dip_domain_port> -D
   weblogic -conDirType IPLANET -conDirUrl <OUD_host>:<oud_port> -conDirBindDN
   <oud_ldap_administrator> -conDirContainer <target_suffix> -backendDirContainer
   cn=products,cn=oraclecontext  -pf <profile_name>
   ```

   The command above creates one import file and one export file with the following naming convention:

   - If the profile name (`-pf argument`) is profile1, `expresSyncSetup` creates the two following profiles `profile1Export` and `profile1Import`.

   To create synchronization profile using EM see refer to the *Administrator's Guide for Oracle Directory Integration Platform*.You can access that document in the Oracle Fusion Middleware 11*g* Release 1 (11.1.1.7) library located at http://www.oracle.com/technetwork/middleware/id-mgmt/documentation/index.html

   Use the DIP graphical user interface to update the list of attributes to be synchronized. This feature is described in the *Administrator's Guide for Oracle Directory Integration Platform*. You can access that document in the Oracle Fusion Middleware 11*g* Release 1 (11.1.1.7) library located at http://www.oracle.com/technetwork/middleware/id-mgmt/documentation/index.html

   Oracle recommends that you create 1-1 exact attribute mappings e.g. cn<->cn and that you create one extra mapping for each attribute alias e.g `commonName->commonName`

7. Configure ACIs

   Additional directory ACIs must be created on the backend directory server for DIP to operate correctly.

   The following command is an example of ACIs created on the backend directory on the suffix to be synchronized (`dc=example,dc=com`):

   ```
   ldapmodify -h <dsee_host> -p <dsee_port> -D "cn=Directory Manager" -w
   <password> <<EOF
   dn: dc=example,dc=com
   changetype: modify
   add: aci
   ```

```
aci: (target="ldap:///dc=example,dc=com")(version 3.0; acl "Entry-level DIP
permissions"; allow (all,proxy)
groupdn="ldap:///cn=dipadmingrp,cn=DIPadmins,cn=Directory Integration
Platform,cn=products,cn=oraclecontext"; allow (all,proxy)
groupdn="ldap:///cn=odipigroup,cn=DIPadmins,cn=Directory Integration
Platform,cn=products,cn=oraclecontext"; )
-
add: aci
aci: (targetattr="*")(version 3.0; acl "Attribute-level DIP permissions"; allow
(all,proxy) groupdn="ldap:///cn=dipadmingrp,cn=DIPadmins,cn=Directory
Integration Platform,cn=products,cn=oraclecontext"; allow (all,proxy)
groupdn="ldap:///cn=odipigroup,cn=DIPadmins,cn=Directory Integration
Platform,cn=products,cn=oraclecontext";)
EOF
```

Export profile's entry must be added to the Export group:

```
ldapmodify -h <dsee_host> -p <dsee_port> -D "cn=Directory Manager" -w
<password> <<EOF
dn: cn=odipegroup,cn=DIPadmins,cn=Directory Integration
Platform,cn=products,cn=oraclecontext
changetype: modify
add: uniqueMember
uniqueMember: orclodipagentname=profile1Export,cn=subscriber
profile,cn=changelog subscriber,cn=directory integration
platform,cn=products,cn=oraclecontext
EOF
```

Note that the profile name (`profile1Export` in the example) is part of the DN of the new member

When two-ways synchronization is used, the Import profile's entry must be added to the Import group:

```
ldapmodify -h <dsee_host> -p <dsee_port> -D "cn=Directory Manager" -w
<password> <<EOF
dn: cn=odipigroup,cn=DIPadmins,cn=Directory Integration
Platform,cn=products,cn=oraclecontext
changetype: modify
add: uniqueMember
uniqueMember: orclodipagentname=profile1Import,cn=subscriber
profile,cn=changelog subscriber,cn=directory integration
platform,cn=products,cn=oraclecontext
EOF
```

In the example above, notice that the profile name (`profile1Export` in the example) is part of the DN of the new member.

8. Managing Directory Bootstrapping.

Bootstrapping refers to the initial transition of data between the (O)DSEE back-end directory and OUD. Because the synchronization process can handle the transition of data between an (O)DSEE and OUD, you are not required to perform directory bootstrapping. However, relying on the synchronization process to perform the initial transition will be a time-consuming process. For this reason, you should perform directory bootstrapping when you first deploy DIP.

There are two possibilities to initialize the two directory topologies:

1. Enable the synchronization so that DIP creates every (O)DSEE entry to OUD.

2. Export the content of the (O)DSEE directory to an LDIF file, then import the content to OUD and configure DIP to use the (O)DSEE changelog.

The first solution is simpler but it is much slower than with the Direct Transition Strategy which uses this procedure.

To use the first solution you must:

1. Enable the synchronization profiles
2. Run the following commands:

```
$ORACLE_HOME/bin/syncProfileBootstrap -h <dip_host> -p <dip_domain_port> -D
weblogic -pf profile1Import

$ORACLE_HOME/bin/syncProfileBootstrap -h <dip_host> -p <dip_domain_port> -D
weblogic -pf profile1Export
```

Directory Boostrapping is described in the *Administrator's Guide for Oracle Directory Integration Platform*. You can access that document in the Oracle Fusion Middleware 11*g* Release 1 (11.1.1.7) library located at http://www.oracle.com/technetwork/middleware/id-mgmt/documentation/index.html

To use the LDIF bootstrapping:

1. Use the following command to export entries from DSEE to `data.ldif` file without the replication metadata and with the backend server in off-line mode:

   ```
   $ dsconf export --no-repl -h host -p port suffix-DN LDIF-file
   ```

2. Retrieve the change number of the last update applied before the export began. To do so, start the export procedure then write down the time and convert it in Generalized Time in YYYYMMDDHHMMSSZ format: An example of a time stamp in a generalized time format is 20130508200557Z, which specifies a time (in the UTC time zone) of 8:05:57 PM on May 28, 2013.
3. Restart the (O)DSEE server (if needed) after the export has completed.
4. Run the following search command:

   ```
   ldapsearch -p <dsee_port> -D <dsee_admin> -w <password> -b "cn=changelog"
   "changetime>= <timeStamp>" changeNumber
   ```

5. Note the value of the smallest changeNumber value returned by doing the following:

   ```
   bash-3.2$ ./ldapsearch -p PORT -h DSEE HOSTNAME -D "cn=directory manager"
   -w PASSWORD -b "cn=changelog" "changetime>=20130508200557Z" changeNumber
   dn: changenumber=16747773,cn=changelog
   changeNumber: 16747773
   dn: changenumber=167477734,cn=changelog
   changeNumber: 167477734
   dn: changenumber=1674777345,cn=changelog
   changeNumber: 1674777345
   ```

6. Use the DIP management console (EM) as described in the "Administering Oracle Directory Integration Platform" section in the *Administrator's Guide for Oracle Directory Integration Platform*.

   You can access that document in the Oracle Fusion Middleware 11*g* Release 1 (11.1.1.7) library located at

http://www.oracle.com/technetwork/middleware/id-mgmt/documentation/index.html

Or you can use the `manageSyncProfiles updatechgnum` command to start synchronization to update the last change number parameters of the DIP synchronization export profile with the above value. The `manageSyncProfiles updatechgnum` command is described in the "Syntax for `manageSyncProfiles`" section of the *Administrator's Guide for Directory Integration Platform.*

You can access that document in the Oracle Fusion Middleware 11*g* Release 1 (11.1.1.7) library located at http://www.oracle.com/technetwork/middleware/id-mgmt/documentation/index.html

7. Enable the DIP synchronization profiles using GUI or CLI as described in the "Enabling and Disabling Synchronization Profiles" section of the *Administrator's Guide for Directory Integration Platform.*

   You can access that document in the Oracle Fusion Middleware 11*g* Release 1 (11.1.1.7) library located at http://www.oracle.com/technetwork/middleware/id-mgmt/documentation/index.html

Synchronization will now begin based on the changelog.

4.8 Step 7: Deploying Replicated Topology

Once the OUD reference instance is initialized, most of the transition work is completed.

Additional instances are created and initialized with the batch procedure identified in Section 4.5, "Step 4: Transitioning Directory Configuration." Replication is then enabled between OUD instances.

More information is located at: *Administering Oracle Unified Directory Guide*, and *Installing Oracle Unified Directory Guide*.

Once a reference OUD server has been configured and loaded with data from (O)DSEE as indicated in: "Step 1: Creating a Reference OUD Instance," "Step 2: Using ds2oud to Diagnose the (O)DSEE Directory Server, Configuration, Schema and Data," "Step 3: Transitioning Directory Schema," "Step 4: Transitioning Directory Configuration", additional instances can be set up in the replicated environment. This step covers:

1. Configuring an OUD Replica
2. Deploying Topology
3. Initializing Data

These steps are required for every strategy.

Types of Replicas

As a reminder, (O)DSEE makes the distinction between three types of replicas:

1. A **master replica** is a read-write database that contains a master copy of the directory data.
2. A **consumer replica** is a read-only database that contains a copy of the information held in a master replica.
3. A **hub replica** is a read-only database, like a consumer replica, but stored on a directory server that supplies one or more consumer replicas.

For more information on (O)DSEE replicas, refer to the "Introduction to Replication" section in the *Oracle Directory Server Enterprise Edition Reference*. That document can be found in the Oracle Directory Server Enterprise Edition 11*g* Release 1 (11.1.1.5) library at
http://www.oracle.com/technetwork/middleware/id-mgmt/documentation/index.html

The OUD replication model is a multi-master model. In other words, all directory server replicas in a replicated topology can process both read and write operations.

Since the release of DSEE 6.x we have recommended multi-master replica with typical deployments which eliminated the need for consumer and hub replicas.

In most deployments, using read-only replica is not needed for performance reason and should only be done if the applications require it. In this case it is achieved by configuring the writability mode of the backend. However, you can configure an OUD directory server to be read-only, in which case add, modify, and delete operations from LDAP clients are rejected on this server and a referral is returned containing pointers to others (read-write) servers within the replicated topology.

Configuring an OUD Read-Write Replica

- Cascaded Replication vs. Centralized Replication Model

  In (O)DSEE, hub replicas are introduced with cascaded replication to make the replication protocol operate better. Cascading replication is useful in the following scenarios:

  - When there are a lot of consumers.
  - Because the masters in a replication topology handle all update traffic, it could put them under a heavy load to support replication traffic to the consumers. You can off-load replication traffic to several hubs that can each service replication updates to a subset of the consumers.
  - To reduce connection costs by using a local hub in geographically distributed environments.

  In OUD, hub replicas do not exist. Replication is built around a centralized publish-subscribe architecture. Each directory server communicates with a central service, and uses the central service to publish its own changes and to receive notification about changes on other directory servers. This central service is called the replication service. OUD read-write masters are the default so in most cases they are deployed.

  The replication service can be made highly available by using multiple server instances running on multiple hosts. Within the replication architecture, a server instance that provides the replication service is called a replication server. A server instance that provides the directory service is called a directory server.

  In a small topology (up to four directory servers) it makes sense to configure each server to function as both a directory server and a replication server. In a large topology (more than twenty directory servers) it is advisable to separate the directory server and replication server instances into separate JVMs, and to limit the number of replication servers.

  Between these two extremes, you can decide on the configuration that works best for your requirements. Having all servers functioning as both directory servers and replication servers is generally a simpler topology and easier to administer. Separating the directory servers and replication servers lowers the disk

requirements of the directory server instances because they do not need to store a replication change log.

In large topologies with several directory servers and several replication servers, it is more efficient to spread the directory servers out across the replication servers in a predefined manner. This is particularly important if the replication servers are running on different types of machines with different capabilities. If the estimated performance of the machines differs significantly from one replication server to another, it is useful to balance the load on the replication servers according to their power.

You must understand the replication concepts of OUD because they are different than those of (O)DSEE. For more information about configuring Replication Servers and Load-balancing, refer to the "Replication Server Load Balancing" section in the *Administering Oracle Unified Directory Guide.* That document can be can be found in the Oracle Unified Directory 11*g* Release 2 (11.1.2) library at http://www.oracle.com/technetwork/middleware/id-mgmt/documentation/index.html

Configuring an OUD Read-Only Replica

This example assumes a replication configuration with replication servers on two hosts: host1 and host2. The example makes the directory server on host2 a read-only replica and uses the `dsconfig` command which accesses the server configuration using the administration connector.

For more information on configuring an OUD read-only replica, see the "Managing Administration Traffic to the Server" section in the *Administering Oracle Unified Directory Guide*. That document can be found in the Oracle Unified Directory 11*g* Release 2 (11.1.2) library at http://www.oracle.com/technetwork/middleware/id-mgmt/documentation/index.html

To configure OUD as a read-only replica use the `dsconfig` command to set the writability-mode of host2:

```
$ dsconfig -h host2 -p 4444 -D "cn=Directory Manager" -j <password_file> -X -n
\
  set-global-configuration-prop --set writability-mode:internal-only
```

A writability mode of internal-only means that replication operations are processed on the server, but the server is not writable directly by LDAP client applications.

Deploying Servers

To create new OUD instances and enable replication between them do the following:

1. Create an OUD instance. For instructions for setting up a directory server refer to: the *Installing Oracle Unified Directory Guide*.
2. Configure each OUD instance by applying the configuration changes identified in Section 4.5, "Step 4: Transitioning Directory Configuration," and for the additional configuration changes that might have been identified while importing the data, see: Section 4.6, "Step 5: Transitioning User Data and Directory Metadata."
3. Run the `dsreplication` command to enable replication between OUD instances. The `dsreplication` command is described in the "To Enable Replication Between Two Servers" section of the *Administrator's Guide for Oracle Unified Directory*. That document can be found in the Oracle Unified Directory 11*g* Release 2 (11.1.2) at http://www.oracle.com/technetwork/middleware/id-mgmt/documentation/index.html

Deploying servers in a replicated topology is described in the "Configuring Data Replication With dsreplication" section in the *Administering Oracle Unified Directory Guide.* That document can be found in the Oracle Unified Directory 11*g* Release 2 (11.1.2) at
http://www.oracle.com/technetwork/middleware/id-mgmt/documentation/index.html

Once an OUD server is loaded with (O)DSEE data, you can either import the same file on every other OUD instance or use binary copy or initialize a replicated server with the data from another replicated server as described in the *Administering Oracle Unified Directory Guide*.

Initialize OUD with (O)DSEE Data

Once you have set up the replication topology, you will need to initialize it with fresh data. There are four different options for every strategy to initialize the OUD instance with the (O)DSEE data already contained in the reference instance.

If you are using the Replication Gateway Strategy, you must ensure that the OUD reference instance is loaded with (O)DSEE data that was exported before the (O)DSEE replication purge delay configured on (O)DSEE.

The four options are:

- Run the `dsreplication` command to initialize each empty OUD instance. This procedure in described in section "26.1.2" of the *Administering Oracle Unified Directory Guide*.
- Initialize each OUD instance at the same time. This procedure is describe in *Section 26.1.3 of the Administering Oracle Unified Directory Guide*.
- Perform a binary copy of the database files from the reference OUD to each OUD instance. This procedure is described in *Section 26.4.3 of the Administering Guide Oracle Unified Directory Guide*.
- Export entries from the reference OUD and reimported them into each empty OUD instance.

4.9 Step 8: Redirecting Traffic to the OUD Topology

Coexistence between the two environments is kept until the application testing is complete.

This procedure depends on the architecture. Redirection may involve the reconfiguration of the software or hardware load-balancers, LDAP proxy servers, modification of the Domain Name Systems (DNS), or use of IP impersonation.

4.10 Step 9: Stopping Coexistence

When all the applications have been redirected to OUD and validated, the Replication Gateway(s) and companion (O)DSEE server can be deprovisioned.

Once the Replication Gateway is no longer in use, it can be stopped and then uninstalled and the same is true for the (O)DSEE side.

Note: After performing Section 4.10, "Step 9: Stopping Coexistence," your transition to OUD is complete. If you encounter problems during your transition, contact your Oracle support representative. For more information, go to the My Oracle Support web site located at https://support.oracle.com

5

After the Transition to OUD

This chapter gives information to assist you after your transition from Directory Server Enterprise Edition to Oracle Unified Directory.

This chapter includes the following sections:

5.1 Your New OUD Environment

With its elastic scalability, high availability, superior performance, and enterprise manageability, OUD will deliver carrier grade services that will scale on demand with your business growth. After you conclude your transition to OUD, you can deploy added value features to improve and expand directory services.

OUD with its unique replication gateway, together with DIP and OVD, is the industry's first and only Java-based unified directory solution. It addresses the fragmented solution challenges that enterprises are facing today, significantly reducing total cost of ownership.

Finally, because OUD adheres to the LDAP standards and integrates with Oracle Fusion Middleware platform, your transition to OUD will ensure that your directory service can easily work with existing applications and maximizes the value of data in your directory in a broader Fusion Middleware Solution.

5.2 Additional OUD Information

Refer to the following resources for more information about OUD:

- *Release Notes for Oracle Unified Directory*
- *Administering Oracle Unified Directory*
- *Developer's Guide for Oracle Unified Directory*
- *Installing Oracle Unified Directory*
- The Oracle Directory Services page on the Oracle Technology Network web site located at `http://www.oracle.com/us/products/middleware/identity-management/directory-services/overview/index.html`

A

Transitioning Synchronization Services

This appendix describes how to transition Identity Synchronization for Windows (ISW) configured with Microsoft Active Directory (AD) as the connected directory and Oracle Directory Server Enterprise Edition (ODSEE) as the backend to Oracle Directory Integration Platform (DIP). This section also includes information to configure DIP to synchronize the directory server sources to function as they previously functioned with ISW.

This appendix includes the following sections:

A.1 Understanding the Transition to Oracle Directory Integration Platform

The transition process described in this appendix allows you to replace an existing deployment of Identity Synchronization for Windows with Oracle Directory Integration Platform. The following sections can help you understand and plan this transition:

A.1.1 Transition Components

This transition process covers the following components:

- Identity Synchronization for Windows 6.0 Service Pack 1 11g Release 1

  ISW is a component of Oracle Directory Server Enterprise Edition (ODSEE), formerly Sun Java System Directory Server. ISW includes a set of Core components (configuration directory, console, command-line utilities, system manager, and central logger), individual connectors, connector subcomponents, and Oracle Message Queue.

ISW synchronizes user account information, including passwords, between ODSEE and Microsoft Active Directory. ISW requires two directory server instances: one instance for the user data that is synchronized and another instance for the ISW configuration data.

For more information, see the *Oracle Fusion Middleware Installation and Configuration Guide for Identity Synchronization for Windows 6.0*.

- Oracle Directory Integration Platform 11*g* Release 1 (11.1.1.9.0)

  DIP allows you to integrate your applications and directories, including third-party LDAP directories, with a master back-end directory being ODSEE, Oracle Internet Directory, or Oracle Unified Directory. DIP supports both uni-directional and bi-directional synchronization between ODSEE and Active Directory.

  The DIP back-end directory stores the DIP metadata and also serves as a synchronization endpoint. The DIP metadata information consists of the DIP-specific schema and directory information tree (DIT).

  For more information, see the *Oracle Fusion Middleware Administrator's Guide for Oracle Directory Integration Platform*.

In general, all the steps in the next sections requires compliance with the DIP certification matrix. To view this matrix:

1. Go to the **Oracle Fusion Middleware Supported System Configurations** page:

   `http://www.oracle.com/technetwork/middleware/ias/downloads/fusion-certification-100350.html`

2. Find **System Requirements and Supported Platforms for Oracle Fusion Middleware 11gR1** and open the `xls` file.
3. In the `xls` file, click the **FMW on WLS - Id&Access** tab.

A.1.2 Using This Documentation

The goal of this appendix is to help you configure DIP, so you can synchronize your directory server to have the same functionality you previously had with ISW.

This appendix describes the transition steps to DIP and will help you find the equivalent basic ISW administration tasks in DIP.

This appendix considers only replacing an ISW deployment with DIP. If you also need to transition from ODSEE to OUD, see Chapter 1, "Understanding the Transition to Oracle Unified Directory."

A.1.3 Transition Process

Before the transition, ISW manages the synchronization between the ODSEE and Active Directory source directories. ISW uses one ODSEE instance for the user data that is synchronized and another ODSEE instance to store the ISW configuration data.

The transition process replaces ISW (and its components) with DIP (and its components) and moves the synchronization functionality from ISW to DIP.

After the transition is finished, DIP will manage the synchronization between ODSEE and Active Directory. DIP will then use only one ODSEE instance to store the user data and the DIP metadata that is synchronized. The ODSEE instance that stored the ISW configuration data before the transition will no longer be used.

A.1.4 Where to Find More Information

For more information to help you with the transition, see the following documentation:

- *Oracle Fusion Middleware Administrator's Guide for Oracle Directory Integration Platform*
- *Oracle Fusion Middleware Installation and Configuration Guide for Identity Synchronization for Windows 6.0*
- *Oracle Fusion Middleware Release Notes for Identity Synchronization for Windows 6.0 Service Pack 1*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Directory Server Enterprise Edition*

A.2 Planning the Transition to Oracle Directory Integration Platform

The following sections can help you plan your transition from ISW to DIP:

- Section A.2.1, "Checking Compliance with the DIP Certification Matrix"
- Section A.2.2, "Comparing the ISW and DIP Functionality"
- Section A.2.3, "ISW Parameters to Consider in Planning the Transition"

A.2.1 Checking Compliance with the DIP Certification Matrix

The transition process described in Section A.4, "Executing the Transition to Oracle Directory Integration Platform" requires compliance with the DIP certification matrix.

To find and check the DIP certification matrix, see Section A.1.1, "Transition Components."

A.2.2 Comparing the ISW and DIP Functionality

The following sections provide a comparison of the features and functionality available in ISW and DIP:

- Section A.2.2.1, "ISW Functionality Available in DIP"
- Section A.2.2.2, "ISW Functionalities Not Available in DIP"
- Section A.2.2.3, "DIP Functionalities Not Available in ISW"
- Section A.2.2.4, "DIP Functionality That Requires a Plug-in"

A.2.2.1 ISW Functionality Available in DIP

The following table describes the ISW functionality that is also available in DIP.

Table A–1 Identity Synchronization for Windows Functionality Available in Oracle Directory Integration Platform

Functionality	Identity Synchronization for Windows	Oracle Directory Integration Platform
Synchronization scope	ISW supports Synchronization User Lists (SULs) that are the smallest synchronization units. An SUL contains a base DN from ODSEE and Active Directory that is mapped for synchronization. One or more SULs can be created under a single domain.	DIP supports domain mapping rules that allow multiple domains (DITs) to be mapped under a base DN. Unlike ISW, DIP has all domains in a single profile share the same filter. However, DIP also allows users to have several profiles with multiple filters.
Direction of synchronization	ISW supports both uni-directional and bi-directional synchronization capabilities.	DIP achieves both uni-directional and bi-directional synchronization capabilities using export and import profiles. The type of profile (export or import) depends on the back-end.
Synchronization change types	ISW supports synchronization of add, modify, and delete operations, selectively. The selection can be modified anytime with the UI.	DIP supports synchronization of all LDAP operations, but it is not possible to select a subset of operation types to synchronize.
Password synchronization	ISW defaults to password synchronization. The synchronization of passwords cannot be avoided.	DIP provides synchronization of all LDAP attributes including user passwords.
User account creation, modification, and delete synchronization	Supported	Supported
User account activation and inactivation	ISW synchronizes account activation/inactivation between Active Directory and ODSEE and vice versa.	DIP synchronizes account activation/inactivation between Active Directory and back end and vice versa.
User account lockout/unlockout synchronization	ISW synchronizes lockout/unlockout events between Active Directory and ODSEE and vice versa. As a pre-requisite, the password policies at both ends are expected to be same.	DIP synchronizes lockout/unlockout events between Active Directory and the back end and vice versa. As a pre-requisite, the password policies at both ends are expected to be same.
Server redundancy	ISW has only one instance, so there is no redundancy.	Multiple instances of DIP can be configured in the WebLogic domain to synchronize the same endpoints. The DIP Quartz Scheduler takes care of providing the failover and load balancing capabilities. However, like ISW, DIP does not provide redundancy when the configuration directory (back-end directory) is not available.
Failover support of endpoints	Supported	DIP does not support failover with ODSEE but does support failover with OUD.
Group synchronization	ISW has special hard-coded handling for group synchronization.	DIP achieves this functionality through a `dnconvert()` function that must be explicitly be added in the attribute mapping rules.
Synchronization with multiple Active Directory domains.	One or more Active Directory connectors can be installed to synchronize with a single ODSEE domain.	DIP achieves this functionality by setting up multiple export and import profiles between different Active Directory domains and the back-end endpoint. DIP also provides a mechanism to handle Foreign Security Principals.

Table A–1 (Cont.) Identity Synchronization for Windows Functionality Available in Oracle Directory Integration Platform

Functionality	Identity Synchronization for Windows	Oracle Directory Integration Platform
Reconciliation of pre-existing entries	ISW uses resynchronization functionality to run a refresh operation that synchronizes the pre-existing entries from ODSEE to Active Directory or vice versa. However, this operation does not synchronize user passwords.	DIP achieves this functionality by resetting the `orclLastAppliedChangeNumber` attribute to some older values, so that the pre-existing entries can be synchronized between the back end to Active Directory and vice versa.
Searchfilter	ISW supports specifying a search filter for each Synchronized User List (SUL).	DIP supports specifying one search filter per profile. You can achieve this filtering using an OR operator in the search filter. You can also have a different profile for a different domain mapping and search filter.
Domain exclusion list	ISW uses a search filter.	DIP supports providing the `DomainExclusionList` to exclude the changes for synchronization.
Logging	ISW supports log per connector and global logs.	DIP supports global logs.

A.2.2.2 ISW Functionalities Not Available in DIP

DIP does not support high availability (HA) with ODSEE.

A.2.2.3 DIP Functionalities Not Available in ISW

DIP supports the following features that are not available in ISW:

Table A–2 DIP Functionalities Not Available in ISW

Feature	ISW	DIP
Attribute Exclusion List	Not supported	DIP provides an `AttributeExclusionList` to exclude synchronizing a specified list of attributes.
Mapping functions	Not supported	DIP supports enhanced attribute mapping with mapping functions that operate on source attribute values to derive the destination attribute values.
Mapping plug-ins	Not supported	DIP allows you to enrich the mapping functions through a Java plug-in mechanism.

A.2.2.4 DIP Functionality That Requires a Plug-in

The following DIP functionality requires the ODSEE plug-in:

- On demand password synchronization from the connected directory (Active Directory) to the backend directory
- Translate password from the backend to the connected directory (Active Directory)

For both of these features, you must install the ODSEE plug-in, which is released with DIP. See "Installing Oracle Directory Server Enterprise Edition Plug-in" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Directory Integration Platform*.

A.2.3 ISW Parameters to Consider in Planning the Transition

Before you begin the transition, consider the ISW parameters and configuration described in the following sections. You will then know if the transition from ISW to DIP will ensure that you have the same level of functionality.

- Section A.2.3.1, "ISW Deployment Considerations"
- Section A.2.3.2, "Planning the Transition"

> **Note:** Carefully read Section A.2.3.1, "ISW Deployment Considerations" and Section A.2.3.2, "Planning the Transition" so you will know if the transition from ISW to DIP will provide you with the same level of functionality, or if you also need to consider a transition from ODSEE to OUD.

A.2.3.1 ISW Deployment Considerations

Before you begin the transition, consider the following ISW parameters and configuration:

- **Synchronization direction of passwords**
  - If passwords are synchronized from Active Directory to Directory Server, you must configure the on-demand password synchronization. See "Password Synchronization" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Directory Integration Platform*.
  - If passwords are synchronized from Directory Server to Active Directory, you must configure the Translate Password feature. See "Password Synchronization" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Directory Integration Platform*.
  - If passwords are synchronized in both directions, both On Demand Password and Translate Password must be configured.

  These features require that you install and configure the ODSEE plug-in. You can find the ODSEE plug-in in one of the following locations in the Oracle Identity Management distribution package, depending on your platform:
  - On Windows systems: `Disk1\utils\dip-plugin\dip-plugin.dll`
  - On UNIX or Linux systems: `Disk1/utils/dip-plugin/dip-plugin.so`

  For more information, see "Installing Oracle Directory Server Enterprise Edition Plug-in" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Directory Integration Platform*.
- **Synchronizing the creation of new users**

  ISW allows you to not synchronize the creation of new users. DIP doesn't make any difference and considers an object creation as a synchronization. If the object doesn't exist, it will be created with the attributes defined in the mapping rules of the profiles. So all the attributes defined as mandatory in the schema need to have a mapping rules in the profile; if not, the first synchronization of the object (that is, creation) will fail.

  See the "Configuring Directory Synchronization" chapter in the *Oracle Fusion Middleware Administrator's Guide for Oracle Directory Integration Platform*.
- **Number of Windows domains**

  There is no limitation in DIP. Many profiles can be created.

- **High Availability** (no changes lost when ISW goes down)

  When ISW is down, Message Queue keeps any changes already read. When ISW is up again, Message Queue and ISW synchronize the changes that occurred when ISW was down.

  To support high availability, DIP is deployed on an Oracle WebLogic Cluster that has at least two servers as a part of the cluster. Oracle WebLogic Cluster starts, stops, and monitors DIP in the cluster. See "Oracle Directory Integration Platform High Availability" in the *Oracle Fusion Middleware High Availability Guide*.

- **Security**

  DIP, as ISW does, can manage connections over SSL, if SSL is required for your deployment.

- **Bidirectional account lockout and unlockout synchronization**

  For these features to work correctly, set the symmetric password policy at both ends (the same as recommended for ISW).

- **Bidirectional group synchronization**

  DIP allows you to manage group synchronization by using the `uniquemenber` attribute and `dnconvert` in the mapping rule.

- **Multi-Master Replication (MMR) Deployment**:

  This item will have consequences in the transition to DIP. If Identity Synchronization for Windows is configured as an MMR deployment, consider the number of Directory Server masters, hubs, and read-only replicas in the deployment.

  In a deployment with multiple Directory Servers, the Identity Synchronization for Windows Directory Server Plug-in must be installed on each master, hub, and read-only replica. When configuring Identity Synchronization for Windows, one Directory Server master is designated as the preferred master. The Directory Server Connector detects and applies changes at the preferred master if it is running. If the preferred master is down, the Connector can optionally apply changes at a second master.

DIP (via WebLogic Cluster) can be configured in high availability (HA) mode, but it will talk to the same ODSEE instance. However, DIP can handle two OUD instances, so if you want to manage the second master, you must also plan a transition from ODSEE to OUD at the same time you are doing the transition from ISW to DIP.

The following table describes the differences in high availability (HA) and multi-master replication (MMR) deployments for ISW and DIP.

Table A–3 Differences for ISW and DIP in HA and MMR Deployments

Function	Identity Synchronization for Windows	Oracle Directory Integration Platform
High Availability (HA)	ISW does not support HA in the true sense. There is only one instance of ISW and if it goes down, no synchronization can be achieved. For other cases, ISW uses Message Queue, which stores the unapplied changes.	DIP deployed on a Oracle WebLogic Cluster can be configured in HA mode. See the *Oracle Fusion Middleware High Availability Guide*.
Multi-Master Replication (MMR)	ISW configuration allows you to specify a preferred and secondary master server. ISW can switch to the secondary server when the preferred server is down.	DIP configuration doesn't allow you to specify two ODSEE servers. However, if OUD is the backend, DIP supports two OUD instances behind a load balancer.

A.2.3.2 Planning the Transition

At this point, you should know which of the following cases you have, and you can plan your transition accordingly:

- Your ISW configuration is not using replicated directory sources, so your plan is to transition ISW to DIP only. See Section A.4, "Executing the Transition to Oracle Directory Integration Platform."
- Your configuration for ODSEE and ISW is in a multi-replicated directory source, so you might have two choices:
  - DIP will talk to your directory server master only, so your plan is to transition ISW to DIP only (same case as above).
  - You want a configuration with two directory server instances, so you must also transition ODSEE to OUD, which must be done before you transition from ISW to DIP. DIP will be then be configured with OUD as the backend.

The following table describes your transition choices.

Table A–4 Planning the ISW to DIP Transition

ISW Configuration	DIP Configuration	Transition to Plan
No replicated directory sources	No replicated directory sources	ISW to DIP
Replicated directory sources	No replicated directory sources	ISW to DIP
Replicated directory sources	Replicated directory sources	ODSEE to OUD and ISW to DIP

The transition from ODSEE to OUD is described in Chapter 1, "Understanding the Transition to Oracle Unified Directory."

The transition from ISW to DIP is described in the Section A.4, "Executing the Transition to Oracle Directory Integration Platform."

A.3 Components Involved in the Different Transition Steps

This section describes the components involved in the transition. Depending on your ISW configuration and the transition case you have selected (see Section A.2.3.2, "Planning the Transition"), the components involved in the transition are different, because the backend can be either ODSEE or OUD.

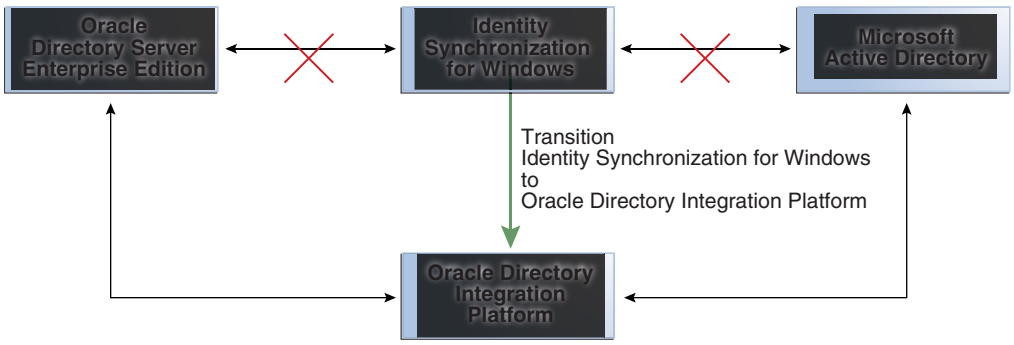
ODSEE is the Backend

If ODSEE is the backend, the following components are involved in the transition, as shown in Figure A–1:

- Source directories that need to be synchronized: ODSEE (backend) and Active Directory (connected directory)
- ISW (and its components) that will be replaced by DIP (and its components)

After the transition, synchronization will be managed by DIP and no longer by ISW. The directory servers are not changed.

Figure A–1 Components Involved in the Transition from ISW to DIP When ODSEE is the Backend



OUD is the Backend

If OUD is the backend, the transition from ODSEE to OUD has already been done, and you are in an intermediate situation where ISW is synchronizing changes between Active Directory and ODSEE. ODSEE is replicated to OUD with one of the strategies described in Section 1, "Understanding the Transition to Oracle Unified Directory." DIP will be configured with OUD as the backend, and the components and the transition process are the same as described above, except for the directory backend.

A.4 Executing the Transition to Oracle Directory Integration Platform

This section describes the tasks to perform the transition from ISW to DIP, including:

- Step 1: Collect Identity Synchronization for Windows Information
- Step 2: Backing Up the Backend Directory Data
- Step 3: Install Oracle Directory Integration Platform
- Step 4: Configure Oracle Directory Integration Platform
- Step 5: Create Synchronization Profiles
- Step 6: Create a Profile for Metadata Creation in Existing ODSEE Entries
- Step 7: Stop the Synchronization on Identity Synchronization for Windows

- Step 8: Uninstall the Identity Synchronization for Windows Plug-in in ODSEE
- Step 9: Update the Metadata in ODSEE by Running the DIP Tester Utility
- Step 10: Enable the Profiles in DIP
- Step 11: Check for Any Remaining Changes in Identity Synchronization for Windows
- Step 12: Check the Synchronization

A.4.1 Step 1: Collect Identity Synchronization for Windows Information

The purpose of this section is to help you collect all the ISW information needed to configure DIP. Fill in the tables in the following sections to order the data and to be able to create the DIP profiles:

- Section A.4.1.1, "Using the Identity Synchronization for Windows Console"
- Section A.4.1.2, "ISW Servers Connection Information"
- Section A.4.1.3, "Synchronization User Lists"
- Section A.4.1.4, "ISW Configuration: Mapping User Attributes"
- Section A.4.1.5, "Account Disabling"
- Section A.4.1.6, "Synchronization Flow"
- Section A.4.1.7, "Synthesis of ISW Configuration Data"

A.4.1.1 Using the Identity Synchronization for Windows Console

Identity Synchronization for Windows provides an administration Console that centralizes the ISW configuration and administration tasks. You can use the ISW Console to:

- Configure directory sources to be synchronized
- Define mappings for user entry attributes to be synchronized, in addition to passwords
- Specify the users and attributes within a directory or domain topology that will, or will not, be synchronized
- Monitor system status
- Start and stop synchronization

To login to the ISW Console, you must know the Administration Server URL (host name, domain name, and port), administrator (admin) credentials (user ID and password), and the ISW configuration password.

After you log in, you can access the various ISW tasks and configuration tabs to collect the ISW information needed to configure DIP during the transition.

A.4.1.2 ISW Servers Connection Information

If you need information about the ISW Console, see Section A.4.1.1, "Using the Identity Synchronization for Windows Console."

In the ISW Console, identify the following ISW **Directory sources**:

- **Sun Directory Server** on ISW for the DIP **back-end directory** (ODSEE): host, port, user, and password

- **Active Directory** on ISW for the DIP **connected directory** (Active Directory): host, port, user DN, and password.

> **Note:** Clear-text passwords are not retrievable from ISW, so you must get them by other means.

Save this information in a table for the transition to DIP. For example:

Table A–5 Directory Servers for Transition

DIP Server	Host	Non-SSL Port	SSL Port	Admin User	Password
Backend Directory (ODSEE or OUD)	odsee-host	5389	5636	`cn=Directory Manager`	*password1*
Connected Directory (Active Directory)	ad-host	389	636	`cn=Administrator,cn=Users,dc=example,dc=com`	*password2*

A.4.1.3 Synchronization User Lists

For each **Synchronization User List** (SUL) in ISW, identify the following:

- Sun Directory Server (ODSEE), identify the **base DN**: `ou=people,dc=example,dc=com`.
- Windows Directory Source (Active Directory), identify the **base DN**: `cn=users,dc=ad,dc=com` synchronization list

These two base DNs will be translated in DIP as **Domain rules source and destination**. Save this information in a table for the transition to DIP. For example:

Table A–6 Synchronization User Lists for Transition

SUL	Source Domain Name	Destination Domain Name
SUL1	`ou=people,dc=example,dc=com`	`cn=users,dc=ad,dc=com`
SUL2	`ou=people2,dc=example,dc=com`	`ou=isw-people2,dc=ad,dc=com`

Each entry under `ou=people,dc=example,dc=com` and `ou=people,dc=example,dc=com` will be synchronized. The type of object synchronized under this container is determined by the attribute-level mapping rules that follow the DN mapping rules described in the next section.

You can also identify domains to be excluded during synchronization by adding a **`DomainExclusionList`** header in map files and identify domains to be excluded during synchronization.

A.4.1.4 ISW Configuration: Mapping User Attributes

ISW supports two types of attributes:

- **Significant**: attributes that are synchronized between systems when you create or modify user entries.
- **Creation**: attributes that are synchronized between systems only when you create user entries.

DIP synchronizes attributes between systems when you create or modify user entries. If a referenced object class requires the presence of a certain attribute, the object

creation will fail if the attribute is not synchronized. This failure is caused when a mapping rule is not defined in the profile for the attribute. Once an attribute is defined in a mapping rule, it will be synchronized, and the object creation will succeed.

The goal of this section is to collect all the attribute mappings independently of the ISW types (creation and modification) and to sort them in the way that helps to create DIP profiles. So, consider the mapping of the following user attributes in the ISW configuration:

- Section A.4.1.4.1, "Map Attributes for Synchronization"
- Section A.4.1.4.2, "Synchronization Flow"
- Section A.4.1.4.3, "Attributes Modification"
- Section A.4.1.4.4, "Groups Synchronization"

A.4.1.4.1 Map Attributes for Synchronization

If you need information about the ISW Console, see Section A.4.1.1, "Using the Identity Synchronization for Windows Console."

For each attribute listed in the ISW Console **Attributes** tab, map the attribute as shown in the following table:

Table A–7 Attributes to Map for Synchronization

Directory Server Attribute	Active Directory Attribute
uniquemember	member
cn	cn
sn	sn
uid	SAMAccountName
userpassword	unicodepwd

If you are synchronizing passwords (On Demand password or Translate Password) you will need to install the ODSEE plug-in, which is part of DIP delivery, on the ODSEE backend.

For DIP, for each attribute you want to synchronize, you must write a mapping rule. Here is the definition of the attribute mapping rule format:

```
srcAttrName:[ReqAttrSeq]:[SrcAttrType]:[SrcObjectClass]:[dstAttrName]:[DstAttrType
]:[DstObjectClass]:[MappingFuntion]
```

> **Note:** You must write an attribute mapping rule on a single line. If the above definition displays as two lines in your browser or viewer, it is formatting purposes only.

For more information, see "Configuring Mapping Rules" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Directory Integration Platform*.

For examples, see "Supported Attribute Mapping Rules and Examples" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Directory Integration Platform*.

A.4.1.4.2 Synchronization Flow

If you need information about the ISW Console, see Section A.4.1.1, "Using the Identity Synchronization for Windows Console."

From the ISW Console **Object Creation** tab, check the synchronization flow and create tables as follows:

- From the backend (ODSEE or OUD) to Active Directory, you will need to create an export profile. Fill in an export table with the creation attributes.
- From Active Directory to backend (ODSEE or OUD), you will need to create an import profile. Fill in the import table with the creation attributes.

Fill in the following tables below with the creation attributes and their `objectclass`.

Table A–8 Export Table: From ODSEE or OUD to Active Directory

ODSEE or OUD Attribute	Active Directory Attribute
`cn`	`cn`
`uid`	`SAMAccountName`
`userpassword`	`unicodepwd`

Table A–9 Import Table: From Active Directory to ODSEE or OUD

Active Directory Attribute	ODSEE or OUD Attribute
`cn`	`cn`
`SAMAccountName`	`uid`
`unicodepwd`	`userpassword`

A.4.1.4.3 Attributes Modification

If you need information about the ISW Console, see Section A.4.1.1, "Using the Identity Synchronization for Windows Console."

From the ISW Console **Attribute Modification** tab, for each attribute, check the synchronization flow to determine in which table (export, import, or both) you will have to add the attribute mapping.

Special case: Object activation/Inactivation with Active Directory

In ISW, there are three options to synchronize object activation and inactivation with Active Directory:

- Interoperating with Directory Server tools
- Modifying the Directory Server's `nsAccountLock` attribute directly
- Using a custom method for Directory Server

In DIP, account activation and inactivation are configured with the Account Disabling feature. See "Account Disabling Synchronization" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Directory Integration Platform*.

A.4.1.4.4 Groups Synchronization

ISW can be configured to work with "Domain Global Security" as well as "Domain Global Distribution" groups on Active Directory.

In DIP (as with ISW), you must use the following configuration. Map the following Directory Server attributes to Active Directory:

- Directory Server `uid` to Active Directory `SAMAccountName`
- Directory Server `cn` to Active Directory `cn`

If ISW group synchronization is enabled, specific mapping rules must exist in the DIP configuration.

```
# Mapping rules to map groups
cn           : : : groupofuniquenames:cn           : : groupofuniquenames :
member       : : : groupofuniquenames:member       : : orclgroup          :
uniquemember : : : groupofuniquenames:uniquemember : : orclgroup          :
owner        : : : groupofuniquenames:owner        : : orclgroup          :
```

At this point, you should have filled the following tables with attribute mappings:

- An export table (Table A–8, " Export Table: From ODSEE or OUD to Active Directory") that contains attributes synchronized from the backend to Active Directory.
- An import table (Table A–9, " Import Table: From Active Directory to ODSEE or OUD") that contains attributes synchronized from Active Directory to the backend.

If an attribute is synchronized in both directions, a row should exist in both tables.

A.4.1.5 Account Disabling

If the account disabling feature is enabled in ISW, specific mapping rules will be added in DIP.

See "Account Disabling Synchronization" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Directory Integration Platform*.

A.4.1.6 Synchronization Flow

Identify the synchronization flow of your data for the profiles you will need to create in DIP and identify the profiles by giving them a name. For example:

Table A–10 Synchronization Flow of Data for DIP Profiles

Flow Synchronization in ISW	Table Type to Fill	Profile Name	Source	Destination
From the back-end directory to the connected directory	Export	For example: ODSEEToAD	Back-end directory	Connected directory
From the connected directory to the backend directory	Import	For example: ADToODSEE	Connected directory	Back-end directory

A.4.1.7 Synthesis of ISW Configuration Data

The ISW data have been collected and are now ready to be sorted in order to prepare the DIP profiles. Here are the different tables that should have been filled.

Table A–11 Profiles Data for DIP

Flow Synchronization in ISW	Table Type to Fill	Source	Destination
From ODSEE (or OUD) to Active Directory	Export	odsee-host	ad-host

Table A–11 (Cont.) Profiles Data for DIP

Flow Synchronization in ISW	Table Type to Fill	Source	Destination
From Active Directory to ODSEE (or OUD)	Import	ad-host	odsee-host

For an export table, identify the following information:

Table A–12 Export Table Information

Item	ODSEE Source (backend)	Active Directory Destination (connected directory)
Server name: host	odsee-host	ad-host
Server name: port	5389	389
Server name: SSLport	5636	636
Server name: password	*odsee-host-password*	*ad-host-password*
Server name: user	`cn=Directory Manager`	`cn=Administrator,cn=Users,dc=ad,dc=com`
Domain rules	`ou=people,dc=example,dc=com`	`ou=isw-ou,dc=ad,dc=com`
Domain Exclusion List		

Identify the data for the export table and update Table A–13, " Export Attributes Mapping".

Table A–13 Export Attributes Mapping

Source (backend) ODSEE or OUD Attribute Name	Source Attribute Object Class	Destination (connected directory) Active Directory Attribute Name	Destination Attribute Object Class
`ou`	`organizationalUnit`	`ou`	`organizationalUnit`
`cn`	`inetorgperson`	`cn`	`inetorgperson`
`uid`	`inetorgperson`	`SAMAccountName`	`user`
`mail`	`inetorgperson`	`mail`	`user`
`sn`	`person`	`sn`	`user`

Use Table A–14, " ISW Features Enabled in Direction Backend to Active Directory (Export)" to list the features that need to be translated in mapping rules in DIP if the features are enabled in ISW.

Table A–14 ISW Features Enabled in Direction Backend to Active Directory (Export)

Feature Enabled in ISW	Yes/No
Password synchronization	yes
Group synchronization	no
Account activation/inactivation	yes

For an import table, identify the following information:

Table A–15 Import Table Information

Item	Active Directory Source (connected directory)	ODSEE Destination (backend)
Server name: host	ad-host	odsee-host
Server name: port	389	5389
Server name: SSLport	636	5636
Server name: password	*ad-host-password*	*odsee-host-password*
Server name: user	`cn=Administrator,cn=Users,dc=ad, dc=com`	`cn=Directory Manager`
Domain rules	`ou=isw-ou,dc=ad,dc=com`	`ou=people,dc=example,dc=com`
Domain Exclusion List		

Identify the data for the import table and update Table A–16, " Import Attributes Mapping".

Table A–16 Import Attributes Mapping

Source Active Directory (connected directory) Attribute Name	Source Active Directory Object Class	Destination Backend (ODSEE or OUD) Attribute Name	Destination Backend (ODSEE or OUD) Object Class
`cn`	`user`	`cn`	`inetorgperson`
`SAMAccountName`	`user`	`uid`	`inetorgperson`
`sn`	`user`	`sn`	`person`

Use Table A–17, " ISW Features Enabled in Direction Active Directory to Backend (Import)" to list the features that need to be translated in mapping rules in DIP if the features are enabled in ISW.

Table A–17 ISW Features Enabled in Direction Active Directory to Backend (Import)

Feature Enabled in ISW	Yes/No
Password synchronization	Yes
Group synchronization	No
Account Activation/Inactivation	Yes

Now that you have collected all the information related to your ISW and ODSEE configuration, you must install and configure DIP, as described in the next sections.

A.4.2 Step 2: Backing Up the Backend Directory Data

Caution: In subsequent transition steps, the DIP configuration modifies the schema, and an undo operation is not available. Therefore, Oracle recommends that you backup your existing backend data before you continue.

The backup operation might impact the backend service availability.

To back up your existing ODSEE data:

1. Stop the ODSEE server instance:

   ```
   $ dsadm stop odsee-instance
   ```

2. Backup the ODSEE data:

   ```
   $ dsadm backup odsee-instance ./backup-IDATA
   ```

3. After the backup is completed, start the ODSEE server instance:

   ```
   $ dsadm start odsee-instance
   ```

If you later need to restore the data, use `dsadm restore`.

For more information about ODSEE, see the *Oracle Fusion Middleware Administrator's Guide for Oracle Directory Server Enterprise Edition*.

To backup your OUD data, use the `backup` command. For more information, see "Backing Up and Restoring Data" in the *Oracle Fusion Middleware Administering Oracle Unified Directory*.

A.4.3 Step 3: Install Oracle Directory Integration Platform

You must install Oracle Directory Integration Platform, as described in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

A.4.4 Step 4: Configure Oracle Directory Integration Platform

To configure Oracle Directory Integration Platform:

1. Run the `dipConfigurator setup` command in the Oracle home `bin` directory with the arguments in Table A–18.

Table A–18 `dipConfigurator` Properties for Oracle Directory Server Enterprise Edition

Properties	Description
`wlshost`	Oracle WebLogic Server host name where Oracle Directory Integration Platform is deployed.
`wlsport`	Listening port number of the Oracle WebLogic Managed Server where Oracle Directory Integration Platform is deployed.
`wlsuser`	Oracle WebLogic Server login user name.
`ldaphost`	Oracle Directory Server Enterprise Edition host name, which is `odsee-host`.
`ldapport`	Oracle Directory Server Enterprise Edition server port number. The default value is `636`.
`isldapssl`	Specify `true` or `false` to specify if `ldapport` is SSL or not.
`ldapuser`	The bind DN to connect to the Oracle Directory Server Enterprise Edition.
`isclustered <BOOLEAN>`	Specify if the Oracle Directory Integration Platform instance is in a cluster environment.
`clustercheckininterval <INT>`	Specify the frequency (milliseconds) at which an instance checks for server status (For example, detecting failed instances) with the other instances of the cluster.

For example, on Linux and UNIX systems:

```
$ ORACLE_HOME/bin/dipConfigurator setup -wlshost localhost -wlsport 7001 \
```

```
-wlsuser weblogic -ldaphost odseehost -ldapport 389 -ldapuser \
"cn=Directory Manager" -isldapssl true
```

Or, on Windows systems:

```
C:\> ORACLE_HOME\bin\dipConfigurator setup -wlshost localhost -wlsport 7001 \
-wlsuser weblogic -ldaphost odseehost -ldapport 389 -ldapuser \
"cn=Directory Manager" -isldapssl true
```

2. Configure the Oracle Directory Integration Platform plug-ins by running the `dipConfigurator setupPlugin` command from the command line:

```
$ ORACLE_HOME/bin/dipConfigurator setupPlugin -wlshost localhost \
-wlsport 7001 -wlsuser weblogic -ldaphost odseehost -ldapport 636 -ldapuser \
"cn=Directory Manager" -isldapssl true
```

> **Note:** You can view the `dipConfig.log` file at *ORACLE_HOME* `/ldap/log/dipConfig.log`.

3. Start the Oracle Directory Server Enterprise Edition instance. For example:

```
$ dsadm start instance-path
```

4. Add ACIs by using the `ldapmodify` command. You can derive the suffix (`dn: dc=example,dc=com` in the example) from the information you previously collected. For example, using an LDIF file:

```
$ ldapmodify -h localhost -p 389 -D "cn=Directory Manager" -w password <<EOF
dn: dc=example,dc=com
changetype: modify
add: aci
aci: (target="ldap:///dc=example,dc=com")(version 3.0; acl "Entry-level DIP
permissions"; allow (all,proxy)
groupdn="ldap:///cn=dipadmingrp,cn=DIPadmins,cn=Directory Integration
Platform,cn=Products,cn=oraclecontext"; allow (all,proxy)
groupdn="ldap:///cn=odipigroup,cn=DIPadmins,cn=Directory Integration
Platform,cn=Products,cn=oraclecontext"; )
-
add: aci
aci: (targetattr="*")(version 3.0; acl "Attribute-level DIP permissions"; allow
(all,proxy) groupdn="ldap:///cn=dipadmingrp,cn=DIPadmins,cn=Directory
Integration Platform,cn=Products,cn=oraclecontext"; allow (all,proxy)
groupdn="ldap:///cn=odipigroup,cn=DIPadmins,cn=Directory Integration
Platform,cn=Products,cn=oraclecontext";)
EOF
```

A.4.5 Step 5: Create Synchronization Profiles

The section describes the synchronization profiles creation, using the information you collected in the tables in "Step 1: Collect Identity Synchronization for Windows Information." You can use either the CLI or GUI to create these profiles, as described in the following sections:

- Section A.4.5.1, "Export Profile Creation"
- Section A.4.5.2, "Import Profile Creation"

When you install DIP, template profiles are created for synchronization with the different directory types, including ODSEE. The files used to create the template profiles, as well as property and mapping files, are available in the following directory:

ORACLE_HOME/ldap/odi/conf

> **Note:** After you create these profiles, do not enable them. You will enable them later in a subsequent step.

For more information, see "Creating Synchronization Profiles" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Directory Integration Platform*.

See also "Password Synchronization Mechanism" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Directory Integration Platform*.

A.4.5.1 Export Profile Creation

To create an export profile using the template files in the *ORACLE_HOME*/ldap/odi/conf directory:

1. Make a copy of these export profile template files: activeexport.properties, activeexp.cfg.master, and activeexp.map.master and then rename them as ODSEEToAD.properties, ODSEEToAD.cfg, and ODSEEToAD.map, respectively.
2. Update the ODSEEToAD.properties file, as follows:
   - Profile name: ODSEEToAD
   - Information related to your Active Directory server, such as host and port:
     - odip.profile.condirurl: ad-host.com:636:2
     - odip.profile.condiraccount: cn=Administrator,cn=Users,dc=mat,dc=com

     Copy this information from Table A–12, " Export Table Information".
   - File names for ODSEEToAD.cfg and ODSEEToAD.map:
     - odip.profile.configfile = ODSEEToAD.cfg
     - odip.profile.mapfile = ODSEEToAD.map
   - odip.profile.oidfilter = (no value)
3. Edit the ODSEEToAD.cfg file, as follows:

   Writer: oracle.ldap.odip.gsi.ActiveWriter
4. Update the ODSEEToAD.map file with the correct domain rules. Here is the structure of the map file:

   DomainRules
   %USERBASE%:%USERBASE%:
   AttributeRules
   srcAttrName:[ReqAttrSeq]:[SrcAttrType]:[SrcObjectClass]:[**dstAttrName**]:[DstAttrType]:[DstObjectClass]:[MappingFuntion]

   The %USERBASE% of the DomainRules section will be filled with the info collected in Table A–12, " Export Table Information". For example:

   DomainRules:
   ou=people,dc=example,dc=com :ou=isw-ou,dc=mat,dc=com:

One profile could be created for each ISW SUL, but because a profile contains many domain rules, it is possible to create one profile for many SULs that have the same mapping rules.

The lines in the `AttributesRules` section are the mapping rules. For DIP, for each attribute you want to synchronize from ODSEE (or OUD) to Active Directory, you must write a mapping rule using the mapping rule format described in "Configuring Mapping Rules" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Directory Integration Platform*.

For examples, see also "Supported Attribute Mapping Rules and Examples" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Directory Integration Platform*.

For the data you have collected from your ISW configuration, you must have a mapping rule for each row in Table A–19, " Required Mapping Rules for the Export Profile".

Table A–19 Required Mapping Rules for the Export Profile

Source (backend)		**Destination (connected directory)**	
ODSEE or OUD Attribute Name	**Source Attribute Object Class**	**Active Directory Attribute Name**	**Destination Attribute Object Class**
ou	organizationalUnit	ou	organizationalUnit
cn	inetorgperson	cn	inetorgperson
uid	inetorgperson	SAMAccountName	user
mail	inetorgperson	mail	user
sn	person	sn	user

For example, here are the mapping rules for this table:

```
# Organizational unit mapping
ou    : : :organizationalunit:ou        : :organizationalunit :
cn    : : :inetorgperson:cn             : :inetorgperson      :
uid   : : :inetorgperson:SAMAccountName : :user               :
mail  : : :inetorgperson:givenname      : :user               :
sn    : : :person:sn                    : :user               :
```

Here are considerations for writing the mapping rules in Table A–14, " ISW Features Enabled in Direction Backend to Active Directory (Export)".

- Password Synchronization

  The mapping rule is specific, as it uses a mapping function, `passwordtranslate`.

  ```
  orclodiptranslatepassword : : : :unicodepwd : : user
  :passwordtranslate(orclodiptranslatepassword)
  ```

  For more information, see "Password Synchronization Mechanism" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Directory Integration Platform*.

  If you are synchronizing passwords (Translate Password), you will need to install the ODSEE plug-in, which is part of DIP delivery, on the ODSEE backend. (For OUD, the plug-in is part of OUD). See Section A.4.4, "Step 4: Configure Oracle Directory Integration Platform."

- Group Synchronization

  The following mapping rules must be added:

```
# Mapping rules to map groups
cn           : : :groupofuniquenames:cn           : : groupofuniquenames :
member       : : :groupofuniquenames:member       : : orclgroup          :
uniquemember : : :groupofuniquenames:uniquemember : : orclgroup          :
owner        : : :groupofuniquenames:owner        : : orclgroup          :
```

  See "Supported Attribute Mapping Rules and Examples" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Directory Integration Platform*.

- Account Activation/Inactivation

  The mapping rule is specific, as it is using a mapping function, `AccountDisable ****`. It depends on the backend (the attribute name is different).

  If ODSEE is the backend:

```
nsAccountLock:1:::userAccountControl::user:AccountDisable(nsAccountLock,
"544")
```

  If OUD is the backend:

```
ds-pwp-account-disabled:1:::userAccountControl::user:AccountDisable(ds-pwp-
account-disabled, "544")
```

  See "Account Disabling Synchronization" in the in the *Oracle Fusion Middleware Administrator's Guide for Oracle Directory Integration Platform*.

A.4.5.2 Import Profile Creation

To create an import profile using the example files in the *ORACLE_HOME*/ldap/odi/conf directory:

1. Make a copy of these import profile template files located in *ORACLE_HOME*/ldap/odi/conf: `activechgimp.properties`, `activechgimp.cfg` and `activechgimp.map` and then rename them as `ADToODSEE.properties`, `ADToODSEE.cfg`, and `ADToODSEE.map`, respectively.
2. Update the `ADToODSEE.properties` file, as follows:
   - Profile name: ADToODSEE
   - Information related to your Active Directory server, such as host and port:
     - `odip.profile.condirurl: ad-host.com:636:2`
     - `odip.profile.condiraccount: cn=Administrator,cn=Users,dc=mat,dc=com`

       Copy this information from Table A–15, " Import Table Information".
   - File names for `ADToODSEE.cfg` and `ADToODSEE.map`:
     - `odip.profile.configfile = ADToODSEE.cfg`
     - `odip.profile.mapfile = ADToODSEE.map`
   - `odip.profile.oidfilter = orclObjectGUID`
3. Edit the `ADToODSEE.cfg` file as follows:

   `Reader: oracle.ldap.odip.gsi.ActiveChgReader`

4. Edit the `ADToODSEE.map` file with the correct domain rules.

   The `%USERBASE%` of the `DomainRules` section will be filled with the information collected in Table A–17, " ISW Features Enabled in Direction Active Directory to Backend (Import)". For example:

   ```
   DomainRules
   ou=isw-ou,dc=mat,dc=com:ou=people, dc=example, dc=com :
   ```

   The mapping rules in the `AttributeRules` section are filled with content from Table A–17, " ISW Features Enabled in Direction Active Directory to Backend (Import)". For example:

   ```
   AttributeRules
   # Attribute rules for Windows organizationalunit
   objectguid     : :binary:top  :orclobjectguid:string:orclADObject
   :bin2b64(objectguid)
   cn             : :      : User:cn            :      : inetorgperson :
   sAMAccountName : :      : User:uid           :      : inetorgperson :
   sn             : :      : User:sn            :      : person        :
   ```

   Here are considerations for the writing the mapping rules in Table A–17, " ISW Features Enabled in Direction Active Directory to Backend (Import)".

   - Password Synchronization

     The following mapping rule is specific, because it uses a mapping function, `OnDemandPassword`.

     ```
     pwdLastSet : : : user : orclODIPPwdLastSet : : top :
     onDemandPassword(pwdLastSet)
     ```

     The `orclSourceObjectDN` attribute is needed by the plug-ins. It belongs to several objectClasses: `orclSunOneObject`, `orclADObject`, `orclNDSObject`, `orclOpenLDAPObject`, and `orclTDSObject`. A rule assigning this value must be included in the (import) profile, although the templates already include it. For example:

     ```
     targetdn: : :top:orclSourceObjectDN: :orclADObject:
     ```

     For more information, see "Password Synchronization Mechanism" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Directory Integration Platform*.

     If you are synchronizing passwords (OnDemand Password feature), you will need to install the ODSEE plug-in, which is part of DIP delivery, on the ODSEE backend. (For OUD, the plug-in is part of OUD). See Section A.4.4, "Step 4: Configure Oracle Directory Integration Platform."

   - Group Synchronization

     The following mapping rules must be added:

     ```
     # Mapping rules to map groups
     cn           : : :groupofuniquenames:cn           : :groupofuniquenames :
     member       : : :groupofuniquenames:member       : :orclgroup          :
     uniquemember : : :groupofuniquenames:uniquemember : :orclgroup          :
     owner        : : :groupofuniquenames:owner        : :orclgroup          :
     ```

     See "Supported Attribute Mapping Rules and Examples" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Directory Integration Platform*.

   - Account Activation/Inactivation

The mapping rule is specific, as it is using a mapping function, `AccountDisable ****`. It depends on the backend.

If ODSEE is the backend:

```
userAccountControl:1:::nsAccountLock::top:AccountDisable(userAccountControl
)
```

If OUD is the backend:

```
userAccountControl:1:::ds-pwp-account-disabled::top:AccountDisable(userAcco
untControl)
```

See "Account Disabling Synchronization" in the in the *Oracle Fusion Middleware Administrator's Guide for Oracle Directory Integration Platform*.

A.4.5.3 General Remarks About DIP Profiles

Several considerations about DIP profiles are:

- One DIP profile must be created for one ISW Synchronization User List (SUL).
- One DIP profile is for one direction: source to destination. If synchronization is done in both directions, two profiles must be created and associated.

A.4.6 Step 6: Create a Profile for Metadata Creation in Existing ODSEE Entries

This profile will be used to create all of the metadata used by DIP in the existing entries of ODSEE.

The metadata is normally created during synchronization or during bootstrap; however, because the metadata in ODSEE has not been created with either of these operations, it must be added in the existing entries.

This profile will be created to be used once, just after the synchronization stop on ISW and before the synchronization start on DIP. This profile will add the metadata in the entries that have been synchronized with ISW.

When you install DIP, template profiles are created for synchronization with the different directory types, including ODSEE. The files used to create the template profiles, as well as property and mapping files, are available in the following directory:

ORACLE_HOME`/ldap/odi/conf`

To create a profile for the metadata using the template files in the *ORACLE_HOME*`/ldap/odi/conf` directory:

1. Make a copy of these template profile files: `activechgimp.properties`, `activechgimp.cfg`, and `activechgimp.map`, and then rename them as `MetaDataImp.properties`, and `MetaDataImp.cfg`, and `MetaDataImp.map`, respectively.
2. Update the `MetaDataImp.properties` file as follows:
   - Profile name: MetaDataImp
   - Paths of the `MetaDataImp.cfg` and `MetaDataImp.map` files
   - Following flag:

     ```
     odip.profile.updateChangeNumberatCreate = false
     ```

     If this flag is set to `true`, the Last Change Number attributes are updated with the current time stamp.

3. Modify the `MetaDataImp.cfg` file as follows:

```
[INTERFACEDETAILS]
Reader: oracle.ldap.odip.gsi.ActiveChgReader
```

4. In the `MetaDataImp.map` file, modify the domain mapping rules based on your data and requirements that you collected in Table A–15, " Import Table Information". Here is the mapping rule format:

```
DomainRules
%USERBASE%:%USERBASE%:
AttributeRules
srcAttrName:[ReqAttrSeq]:[SrcAttrType]:[SrcObjectClass]:[dstAttrName]:[DstAttrT
ype]:[DstObjectClass]:[MappingFuntion]
```

A profile could have many Domain Rules, so we could create one profile for many SULs.

For DIP, for each attribute you want to synchronize from ODSEE (or OUD) to Active Directory, you must write a mapping rule using mapping rule format.

For more information, see "Configuring Mapping Rules" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Directory Integration Platform*.

For examples, see "Supported Attribute Mapping Rules and Examples" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Directory Integration Platform*.

So, regarding the data you have collected from your ISW configuration, for each line in Table A–15, " Import Table Information", you must have a mapping rule.

Notes

- The domain rules must be updated with the data you have collected from the ISW configuration.

  The `%USERBASE%` of the `DomainRules` section will be filled with the information you collected in Table A–15, " Import Table Information". For example:

```
DomainRules
ou=isw-ou,dc=ad,dc=com:ou=people,dc=example,dc=com
```

- The following mapping rules are mandatory:

```
objectguid: :binary:top:orclobjectguid:string:orclADObject:bin2b64(objectguid)
distinguishedName: : :top:orclSourceObjectDN: :orclADObject:
```

- The `odip.profile.updateChangeNumberatCreate` flag should be set to `false`.

The profile will be enabled after the synchronization is stopped for ISW.

A.4.7 Step 7: Stop the Synchronization on Identity Synchronization for Windows

It is strongly recommended that you stop the ISW server. At least, plan for a decrease of activity on both Active Directory and ODSEE, and then stop the synchronization on ISW.

Note: Be sure to note the value of the last change number that has been applied, because it will be used in the last step to check that no changes have been lost.

To stop the synchronization, open a terminal window (or a Command Window) and type the `idsync stopsync` command. For example:

```
$ idsync stopsync -w admin-password -q configuration_password
```

A.4.8 Step 8: Uninstall the Identity Synchronization for Windows Plug-in in ODSEE

Before you uninstall the ISW plug-in, check for any existing entries in ODSEE that still require a bind (On-Demand Password synchronization). To find these entries, use `ldapsearch` to check for:

- The `userPassword` attribute has the following value:

  ```
  userPassword: {PSWSYNC}*ON-DEMAND*SYNCHRONIZATION*REQUIRED*
  ```

  and/or

- The `dspswvalidate` attribute is set to `true`.

If you find entries that still require a bind, add the `orclODIPInvalidPassword` attribute (value is `true`) to every entry where the `dspswvalidate` attribute is set to `true`. The bind will then be performed by the DIP ODSEE plug-in.

Then, you can uninstall the ISW plug-in.

To unconfigure the ISW plug-in, open a terminal window (or a Command Window) and type the `idsync dspluginconfig` command. For example:

```
$ idsync dspluginconfig -U -w admin password -q configuration_password
```

Or, use `ldapmodify`:

```
$ ldapmodify -h host.example.com -p 5389 -D "cn=Directory Manager" -w
admin-password
dn: cn=pswsync,cn=plugins,cn=config
changetype: modify
replace: nsslapd-pluginEnabled
nsslapd-pluginEnabled:off
```

Restart the ISW server, and then remove the `dspswvalidate` attribute from the entries.

A.4.9 Step 9: Update the Metadata in ODSEE by Running the DIP Tester Utility

The ODSEE entries that have been created through a synchronization done with ISW don't contain the metadata needed by DIP.

> **Note:** In a typical DIP/ODSEE configuration, the entries are created during synchronization or during bootstrap and contain the metadata needed by DIP. In the current case, the user entries have not been created with one of these operations but synchronized with ISW, and therefore, they don't contain the metadata.

To add this metadata, a profile must be created and used once. No synchronization will trigger this profile execution, so you must run DIP Tester either through Oracle Enterprise Manager Fusion Middleware Control or the CLI (using `manageSyncProfile -testProfile`). This profile must also be registered first.

Register the profile using `manageSyncProfiles`:

```
$ manageSyncProfiles register -h $WLSHOST -p 7005 -D weblogic -f
```

```
MetaDataImp.properties -pf MetaDataImp
```

Then, run DIP Tester using either Oracle Enterprise Manager Fusion Middleware Control:

- In the Advanced tab, set `lastChangeNumber` to 0.
- In the Filtering tab, the Source Matching Filter and Destination Matching Filter should be unset.

Or, run `manageSyncProfile` from the command line:

```
$ manageSyncProfile -testProfile -h $WLSHOST -p 7005 -D weblogic -pf MetaDataImp
-changenumber 0
```

The entries that were previously synchronized with ISW are now ready to be synchronized with DIP, and the profile can be deleted.

For more information, see:

- "Troubleshooting Synchronization Profiles Using DIP Tester" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Directory Integration Platform*
- "Managing Synchronization Profiles Using `manageSyncProfiles`" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Directory Integration Platform*

A.4.10 Step 10: Enable the Profiles in DIP

The synchronization is activated in DIP when the profiles are registered and enabled.

To register, associate, and enable the profiles:

1. Register the profiles:

   ```
   $ ORACLE_HOME/bin/manageSyncProfiles register -h $myWLSHOST -p 7005 \
   -wlsuser weblogic -pf ODSEEToAD -file ODSEEToAD.properties

   $ ORACLE_HOME/bin/manageSyncProfiles register -h $myWLSHOST -p 7005 \
   -wlsuser weblogic -pf ADToODSEE -file ADToODSEE.properties
   ```

2. If the data is synchronized in both directions and you have export and import profiles for the same source and destination, you must also associate the two profiles. This association prevents loops from occurring in bi-directional synchronization where changes initiated from one directory return to the same directory.

   Associate the profiles:

   ```
   $ ORACLE_HOME/bin/manageSyncProfiles associateProfile -h $myWLSHOST -p 7005 \
   -wlsuser weblogic -pf ODSEEToAD -assopf ADToODSEE

   $ ORACLE_HOME/bin/manageSyncProfiles associateProfile -h $myWLSHOST -p 7005 \
   -wlsuser weblogic -pf ADToODSEE -assopf ODSEEToAD
   ```

3. Enable the profiles (synchronization will start once the profiles are enabled):

   ```
   $ ORACLE_HOME/bin/manageSyncProfiles activate -pf ODSEEToAD

   $ ORACLE_HOME/bin/manageSyncProfiles activate -pf ADToODSEE
   ```

For more information, see "Managing Directory Synchronization Profiles" the *Oracle Fusion Middleware Administrator's Guide for Oracle Directory Integration Platform*.

A.4.11 Step 11: Check for Any Remaining Changes in Identity Synchronization for Windows

Some changes might have occurred while ISW synchronization was stopped. Check that the last change number of your source has been applied on the destination.

DIP Tester allows you to perform synchronization tests and to return detailed log messages generated during the tests. See "Troubleshooting Synchronization Profiles Using DIP Tester" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Directory Integration Platform*.

A.4.12 Step 12: Check the Synchronization

To verify that the synchronization is working correctly, modify an attribute on one server and check that it is correctly synchronized on the other server.

> **Note:** The On-Demand Password synchronization feature should be working in the same way it was working with ISW. When a password is modified in Active Directory, the `orclODIPInvalidPassword` attribute is added and set to `true` in the ODSEE entry, and a bind is required to update the `userPassword` attribute.

A.5 Basic Administration Tasks

Table A–20 describes some basic administrative tasks in ISW and how you perform the equivalent tasks in DIP. Here are documentation references for performing the DIP tasks in this table:

- Enterprise Manager refers to Oracle Enterprise Manager Fusion Middleware Control. For more information, see "Managing Oracle Directory Integration Platform Using Fusion Middleware Control" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Directory Integration Platform* or the Enterprise Manager online Help.
- For information about `manageSyncProfiles`, see "Managing Synchronization Profiles Using `manageSyncProfiles`" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Directory Integration Platform*.
- For information about the WebLogic Scripting Tool and the WebLogic Administration Console, see *Oracle Fusion Middleware Managing Server Startup and Shutdown for Oracle WebLogic Server*.

Table A–20 Basic Administrative Tasks in ISW and DIP

ISW Task	Equivalent DIP Task	Command-Line	GUI
Configuring directory sources	Edit or create profile	`manageSyncProfiles`	Enterprise Manager
Configuring synchronization settings	Edit or create profile	`manageSyncProfiles`	Enterprise Manager
Configuring attribute settings	Edit or create profile	`manageSyncProfiles`	Enterprise Manager
Configuring attribute modification settings	Edit or create profile	`manageSyncProfiles`	Enterprise Manager
Configuring group synchronization settings	Edit or create profile	`manageSyncProfiles`	Enterprise Manager
Configuring synchronization user lists (SULs)	Edit or create profile	`manageSyncProfiles`	Enterprise Manager

Table A–20 (Cont.) Basic Administrative Tasks in ISW and DIP

ISW Task	Equivalent DIP Task	Command-Line	GUI
Installing connectors and initializing data (`idsync` command)	Not applicable	Not applicable	Not applicable
Starting and stopping synchronization	Register and activate profile	`manageSyncProfiles`	Enterprise Manager
Starting and stopping services (ISW and Message Queue)	Start and stop WebLogic Server	WebLogic Scripting Tool, scripts	WebLogic Admin Console

DIP also has the following tools to test synchronization profiles:

- DIP Tester: Use this utility to perform synchronization tests and to return detailed log messages generated during the tests. See "Troubleshooting Synchronization Profiles Using DIP Tester" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Directory Integration Platform*.
- Log Level: Specify the logging level for debugging synchronization profiles using Oracle Enterprise Manager Fusion Middleware Control. See "Creating Synchronization Profiles" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Directory Integration Platform*.

A.6 After the Transition to Oracle Directory Integration Platform

In case you have considered only the transition to DIP and your backend is still ODSEE, you might reconsider transitioning ODSEE to OUD in a second step.

In you transition ODSEE to OUD, OUD will be considered as a fresh installation, and you will have to create new profiles with OUD as the server instead of ODSEE. The new profiles will be similar to ODSEE profiles, but the main changes will be connection information such as server names and port numbers. Some attribute names and values might also have to be updated.

For more information, see Chapter 1, "Understanding the Transition to Oracle Unified Directory."