Oracle® Collaboration Suite

Integration with Microsoft Active Directory

Release 2 (9.0.4) for Solaris

Part No. B15610-01

November 2004

ORACLE®

Oracle Collaboration Suite Integration with Microsoft Active Directory, Release 2 (9.0.4) for Solaris

Part No. B15610-01

Primary Author: Karen Mullally

Contributing Author: Julia Pond, Richard Smith, Henry Abrecht

Contents

2 Integration with the Microsoft Windows Environment

3 Windows Native Authentication

Index

Send Us Your Comments

Oracle Collaboration Suite Integration with Microsoft Active Directory, Release 2 (9.0.4) for Solaris

Part No. B15610-01

Oracle welcomes your comments and suggestions on the quality and usefulness of this publication. Your input is an important part of the information used for revision.

- Did you find any errors?
- Is the information clearly presented?
- Do you need more information? If so, where?
- Are the examples correct? Do you need more examples?
- What features did you like most about this manual?

If you find any errors or have any other suggestions for improvement, please indicate the title and part number of the documentation and the chapter, section, and page number (if available). You can send comments to us in the following ways:

- Electronic mail: ocsdocs_us@oracle.com
- FAX: (650) 506-7410. Attn: Oracle Collaboration Suite Documentation Manager
- Postal service:

  Oracle Corporation
  Oracle Collaboration Suite Documentation
  500 Oracle Parkway, M-S 2OP5
  Redwood Shores, CA 94065
  USA

If you would like a reply, please give your name, address, telephone number, and electronic mail address (optional).

If you have problems with the software, please contact your local Oracle Support Services.

Preface

Microsoft Active Directory can be used in place of Oracle Collaboration Suite Identity Management to manage identities on your Oracle Collaboration Suite Release 2 (9.0.4) deployment. In order to use Microsoft Active Directory with Oracle Collaboration Suite, you must integrate Microsoft Active Directory with Oracle Application Server 10*g (9.0.4)*.

This book consolidates existing Oracle documentation that describes the procedures necessary to integrate Microsoft Active Directory with Oracle Application Server 10*g (9.0.4)*.

To successfully integrate Microsoft Active Directory into your Oracle Collaboration Suite 9.0.4 deployment, complete the tasks described in this book in chapter order. See "Organization" below.

This preface contains the following topics.

> **Note:** The information in this document is accurate to the best of our knowledge at the time of publication. You can access the latest information on the Oracle Technology Network at `http://otn.oracle.com`.

Audience

This book is intended for Oracle Collaboration Suite Release 2 (9.0.4) users interested in integrating Microsoft Active Directory with Oracle Collaboration Suite.

Organization

This book contains the following chapters.

Related Documentation

The following documents provide additional information on Oracle Collaboration Suite and can be located at:

http://otn.oracle.com

Oracle Database Documents

Oracle9i Database Administrator's Guide

Oracle Application Server Documents

Oracle Application Server 10g Upgrading to 10g (9.0.4) Guide
Oracle Application Server Administrator's Guide

Management and Security Documents

Oracle Application Server Single Sign-On Administrator's Guide 10g (9.0.4)
Oracle Internet Directory Administrator's Guide

Conventions

This section describes the conventions used in the text and code examples of this documentation set. It describes:

- Conventions in Text
- Conventions in Code Examples
- Conventions for Windows Operating Systems

Conventions in Text

We use various conventions in text to help you more quickly identify special terms. The following table describes those conventions and provides examples of their use.

Convention	Meaning	Example
Bold	Bold typeface indicates terms that are defined in the text or terms that appear in a glossary, or both.	When you specify this clause, you create an **index-organized table**.
Italic	Italic typeface indicates book titles or emphasis.	*Oracle10g Database Concepts* Ensure that the recovery catalog and target database do not reside on the same disk.
`UPPERCASE monospace (fixed-width) font`	Uppercase monospace typeface indicates elements supplied by the system. Such elements include parameters, privileges, datatypes, RMAN keywords, SQL keywords, SQL*Plus or utility commands, packages and methods, as well as system-supplied column names, database objects and structures, usernames, and roles.	You can specify this clause only for a `NUMBER` column. You can back up the database by using the `BACKUP` command. Query the `TABLE_NAME` column in the `USER_TABLES` data dictionary view. Use the `DBMS_STATS.GENERATE_STATS` procedure.

Convention	Meaning	Example
`lowercase monospace (fixed-width) font`	Lowercase monospace typeface indicates executables, filenames, directory names, and sample user-supplied elements. Such elements include computer and database names, net service names, and connect identifiers, as well as user-supplied database objects and structures, column names, packages and classes, usernames and roles, program units, and parameter values. **Note:** Some programmatic elements use a mixture of UPPERCASE and lowercase. Enter these elements as shown.	The password is specified in the `orapwd` file. Back up the datafiles and control files in the `/disk1/oracle/dbs` directory. The `department_id, department_name`, and `location_id` columns are in the `hr.departments` table. Set the QUERY_REWRITE_ENABLED initialization parameter to true. Connect as `oe` user. The `JRepUtil` class implements these methods.
`lowercase italic monospace (fixed-width) font`	Lowercase italic monospace font represents placeholders or variables.	You can specify the *`parallel_clause`* *`Run Uold_release.SQL`* where *`old_release`* refers to the release you installed prior to upgrading.
Text within angle brackets `< >`	Angle brackets represent variables in the Oracle Calendar sections of this document.	Enter the `<hostname>`, `<port>`.

Conventions in Code Examples

Code examples illustrate SQL, PL/SQL, SQL*Plus, or other command-line statements. They are displayed in a monospace (fixed-width) font and separated from normal text as shown in this example:

```
SELECT username FROM dba_users WHERE username = 'MIGRATE';
```

The following table describes typographic conventions used in code examples and provides examples of their use.

Convention	Meaning	Example
[ ]	Brackets enclose one or more optional items. Do not enter the brackets.	`DECIMAL (`*`digits`*` [ ,`*`precision`*` ])`
{ }	Braces enclose two or more items, one of which is required. Do not enter the braces.	`{ENABLE | DISABLE}`
|	A vertical bar represents a choice of two or more options within brackets or braces. Enter one of the options. Do not enter the vertical bar.	`{ENABLE | DISABLE}` `[COMPRESS | NOCOMPRESS]`

...	Horizontal ellipsis points indicate either:
	■ That we have omitted parts of the code that are not directly related to the example
	■ That you can repeat a portion of the code
		`CREATE TABLE ... AS subquery;`
		
		`SELECT col1, col2, ... , coln FROM employees;`

Convention	Meaning	Example
. . .	Vertical ellipsis points indicate that we have omitted several lines of code not directly related to the example.	SQL> SELECT NAME FROM V$DATAFILE; NAME ---------- /fs1/dbs/tbs_01.db /fs1/dbs/tbs_02.dbf . . . /fs1/dbs/tbs_09.dbf 9 rows selected.
Other notation	You must enter symbols other than brackets, braces, vertical bars, and ellipsis points as shown.	acctbal NUMBER(11,2); acct CONSTANT NUMBER(4) := 3;
Italics	Italicized text indicates placeholders or variables for which you must supply particular values.	*CONNECT SYSTEM/system_password* *DB_NAME = database_name*
UPPERCASE	Uppercase typeface indicates elements supplied by the system. We show these terms in uppercase in order to distinguish them from terms you define. Unless terms appear in brackets, enter them in the order and with the spelling shown. However, because these terms are not case sensitive, you can enter them in lowercase.	*SELECT last_name, employee_id FROM employees;* SELECT * FROM USER_TABLES; DROP TABLE hr.employees;
lowercase	Lowercase typeface indicates programmatic elements that you supply. For example, lowercase indicates names of tables, columns, or files. **Note:** Some programmatic elements use a mixture of UPPERCASE and lowercase. Enter these elements as shown.	SELECT last_name, employee_id FROM employees; sqlplus hr/hr CREATE USER mjones IDENTIFIED BY ty3MU9;
Text within angle brackets < >	Angle brackets represent variables in the Oracle Calendar sections of this document. Enter the <hostname>, <port>.	%$ORACLE_HOME/bin/ldapmodify -h <host> -p <port> -D cn=orcladmin -w <password> -f index.ldif

Conventions for Windows Operating Systems

The following table describes conventions for Windows operating systems and provides examples of their use.

Convention	Meaning	Example
Choose Start >	How to start a program.	To start the Database Configuration Assistant, choose Start > Programs > Oracle - HOME_NAME > Configuration and Migration Tools > Database Configuration Assistant.

Convention	Meaning	Example
File and directory names	File and directory names are not case sensitive. The following special characters are not allowed: left angle bracket (<), right angle bracket (>), colon (:), double quotation marks ("), slash (/), pipe (|), and dash (-). The special character backslash (\) is treated as an element separator, even when it appears in quotes. If the file name begins with \\, then Windows assumes it uses the Universal Naming Convention.	`c:\winnt"\"system32 is the same as C:\WINNT\SYSTEM32`
C:\>	Represents the Windows command prompt of the current hard disk drive. The escape character in a command prompt is the caret (^). Your prompt reflects the subdirectory in which you are working. Referred to as the command prompt in this manual.	`C:\oracle\oradata>`
Special characters	The backslash (\) special character is sometimes required as an escape character for the double quotation mark (") special character at the Windows command prompt. Parentheses and the single quotation mark (') do not require an escape character. Refer to your Windows operating system documentation for more information on escape and special characters.	`C:\>exp scott/tiger TABLES=emp QUERY=\"WHERE job='SALESMAN' and sal<1600\"` `C:\>imp SYSTEM/`*`password`*` FROMUSER=scott TABLES=(emp, dept)`
HOME_NAME	Represents the Oracle home name. The home name can be up to 16 alphanumeric characters. The only special character allowed in the home name is the underscore.	C:\> net start Oracle*HOME_NAME*TNSListener

Convention	Meaning	Example
ORACLE_HOME and *ORACLE_BASE*	In releases prior to Oracle8i release 8.1.3, when you installed Oracle components, all subdirectories were located under a top level *ORACLE_HOME* directory. For Windows NT, the default location was `C:\orant`. This release complies with Optimal Flexible Architecture (OFA) guidelines. All subdirectories are not under a top level *ORACLE_HOME* directory. There is a top level directory called *ORACLE_BASE* that by default is `C:\oracle`. If you install the latest Oracle release on a computer with no other Oracle software installed, then the default setting for the first Oracle home directory is `C:\oracle\ora`*nn*, where *nn* is the latest release number. The Oracle home directory is located directly under *ORACLE_BASE*. All directory path examples in this guide follow OFA conventions. Refer to *Oracle10i Database Platform Guide* for Windows for additional information about OFA compliances and for information about installing Oracle products in non-OFA compliant directories.	Go to the *ORACLE_BASE**ORACLE_HOME*\rdbms\admin directory.

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible, with good usability, to the disabled community. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For additional information, visit the Oracle Accessibility Program Web site at

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

Accessibility of Code Examples in Documentation JAWS, a Windows screen reader, may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, JAWS may not always read a line of text that consists solely of a bracket or brace

Accessibility of Links to External Web Sites in Documentation This documentation may contain links to Web sites of other companies or organizations that Oracle does

not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

1

Upgrading the Oracle Application Server

In order to use Microsoft Active Directory with Oracle Collaboration Suite, you must integrate Microsoft Active Directory with the Oracle Application Server. The first step in integrating Microsoft Active Directory with Oracle Collaboration Suite is to upgrade the Oracle Collaboration Suite Identity Management Oracle9*i* Application Server 9.0.2.3 to Oracle Application Server 10*g* (9.0.4). This chapter contains the necessary procedures to perform this upgrade.

The following topics guide you through each step of the upgrade procedure:

Oracle Internet Directory-Specific Preupgrade Tasks

This section describes preupgrade tasks required for Oracle Internet Directory.

1. Verify that the `orcladmin` user exists in the default identity management realm, as follows:

   a. Get the default subscriber DN, as follows (the following command is one continuous line):

   ```
   $ORACLE_HOME/bin/ldapsearch -h OID_host -p non-SSL_port -D OID_
   superuser -w OID_superuser_password -b
   "cn=common,cn=products,cn=oraclecontext" -s base "objectclass=*"
   orcldefaultsubscriber
   ```

   b. Get the user nickname and user search base attribute, as follows (the following command is one continuous line):

   ```
   $ORACLE_HOME/bin/ldapsearch -h OID_host -p non-SSL_port -D OID_
   superuser -w OID_superuser_password -b
   "cn=common,cn=products,cn=oraclecontext,default_subscriber_DN" -s
   base "objectclass=*" orclcommonnicknameattribute
   orclcommonusersearchbase
   ```

   c. Search for the `orcladmin` user, as follows (the following command is one continuous line):

   ```
   $ORACLE_HOME/bin/ldapsearch -h OID_host -p non-SSL_port -D OID_
   superuser -w OID_superuser_password -b "user_search_base_DN" -s sub
   "user_nickname_attribute=orcladmin"
   ```

If the last LDAP search does not return anything, create the `orcladmin` user in Oracle Internet Directory, as follows:

a. Create an `ldif` file called `orcl.ldif` that includes the following content:

```
dn: cn=orcladmin, User_Search_Base
changetype: add
uid: orcladmin
mail: orcladmin
givenName: orcladmin
cn: orcladmin
sn: orclAdmin
description: Seed administrative user for subscriber.
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetorgperson
objectClass: orcluser
objectClass: orcluserV2
```

b. Execute the following command (the following command is one continuous line):

```
$ORACLE_HOME/bin/ldapadd -h OID_host -p non-SSL_port -D OID_
superuser -w OID_superuser_password -v -f orcl.ldif
```

2. Verify that the Oracle Internet Directory superuser password conforms to the same restrictions as defined for the Oracle Application Server 10*g* (9.0.4) `ias_admin` user.

> **See Also:** *Oracle Application Server 10g Installation Guide* for more details

If the password does *not* conform to the above restrictions, reset the password so that it conforms to the restrictions, as follows:

a. Create an `ldif` file called `supwd.ldif` that includes the following content:

```
dn:
changetype: modify
replace: orclsupassword
orclsupassword: new_password
```

b. Execute the following command (the following command is one continuous line):

```
$ORACLE_HOME/bin/ldapmodify -h OID_host -p non-SSL_port -D OID_
superuser_DN -w OID_superuser_password -v -f supwd.ldif
```

3. Apply Note 263073.1 available on Oracle*MetaLink* at

`http://metalink.oracle.com`

Backing Up the Oracle Internet Directory

Before proceeding with the upgrade, back up the Oracle Internet Directory database and software.

Preparing to Upgrade the Metadata Repository Database

Before you begin any other Metadata Repository upgrade tasks, perform these steps in the Infrastructure Oracle home.

1. Stop all processes.
2. Back up the database.
3. Install the RDBMS 9.0.1.5 patch set against the Infrastructure Oracle home (if it has not already been installed as part of an Identity Management upgrade). Obtain patch number 3301544 from MetaLink. You need a MetaLink user ID and password to obtain it.
4. Ensure that there are no invalid objects in the database.

   See Also: "Executing the utlrp.sql Utility" on page 1-46 and "Checking for Invalid Database Objects" on page 1-46 for instructions.

5. Obtain the Repository Creation Assistant CD-ROM.
6. Start the database server and listener.
7. Install the DBMS_IAS_UPGRADE package.

   See Also: "Loading the DBMS_IAS_UPGRADE Package" on page 1-3 for instructions.

8. Upgrade the Metadata Repository Container.

   See Also: "Upgrading the Metadata Repository Container" on page 1-4 for instructions.

9. Ensure that there are no invalid objects in the database.

   See Also: "Executing the utlrp.sql Utility" on page 1-46 and "Checking for Invalid Database Objects" on page 1-46 for instructions.

Setting the Environment for Upgrading the Metadata Repository

In order to execute most steps in the Metadata Repository upgrade, it is necessary to set your environment to point to the infrastructure Oracle home. This means setting the ORACLE_HOME environment variable to <*Infra_OH*> and setting the ORACLE_SID environment variable to the instance name for the Infrastructure database. The easiest way to accomplish this is to execute one of the environment scripts, `coraenv` or `oraenv`. `coraenv` can be used to set the environment for `csh` shells. `oraenv` can be used for other shells.

Loading the DBMS_IAS_UPGRADE Package

Before you can upgrade to the Oracle Application Server 10*g* (9.0.4) Infrastructure, you must load a PL/SQL package called `DBMS_IAS_UPGRADE`. This package allows the schema upgrade scripts to grant permissions when they are run as user `SYS`.

Follow these steps to load the package:

1. Ensure that the database and listener are running.
2. Ensure that the ORACLE_HOME environment variable is set to <*Infra_OH*> and the ORACLE_SID environment variable is set to the Infrastructure database SID. If

they are not, follow the instructions in "Setting the Environment for Upgrading the Metadata Repository" on page 1-3.

3. Change directories to `<repCA_CD>/repCA/rdbms/admin`.
4. Connect to SQL*Plus as user `SYS`.
5. Issue these commands:

   `@dbmsiasu.sql`

   `@prvtiasu.plb`

   The following messages appear:

   ```
   Package created.

   Package body created.
   ```

   The PL/SQL package `SYS.DBMS_IAS_UPGRADE` is installed.

Upgrading the Metadata Repository Container

The Metadata Repository Container upgrade process (the `mrc.pl` script) performs two functions:

- Creates new tablespaces and schemas in the metadata repository (`ias_meta`, `wcrsys_ts`, `ocats`, `ip_dt`, `ip_rt`, `ip_idx`, `ip_lob` `OLTS_SVRMGSTORE`, `oltsbattrstore`) tablespaces and `wcrsys`, `oca`, `oraoca_public`, `ip`, `wk_test` and `internet_appserver_registry` schemas).

  Note: If you manually created any of the items listed below after the Oracle9*i*AS Release 2 (9.0.2) Infrastructure installation, then you must move them to a different location, or remove them before you run the Metadata Repository Container upgrade:

  Tablespaces: `ias_meta`, `wcrsys_ts`, `ocats`, `ip_dt`, `ip_rt`, `ip_idx`, `ip_lob`, `OLTS_SVRMGSTORE`, `olts_battrstore`

  Schemas: `wcrsys`, `oca`, `oraoca_public`, `ip`, `wk_test` and `internet_appserver_registry`

  Otherwise, the Metadata Repository Container upgrade will fail. A similar issue is faced by users of the OracleAS RepCA, and is described in detail in the *Oracle Application Server 10g Installation Guide*, sections "Schema Name Already in Use" and Tablespace Name Already in Use".

- Updates the Oracle Internet Directory entry for the repository to accommodate the Release 2 (9.0.4) security architecture

Because the metadata repository and Oracle Internet Directory may reside on different computers, and require different access rights, the script is designed to perform only one of the functions, or both, depending on the credentials given when starting the script.

The Metadata Repository Creation script must be executed before any other schema upgrade scripts are executed, because the new schemas depend on the modifications made by `mrc.pl`.

Depending on the configuration to be upgraded, you will perform one of the following procedures:

- If you have DBA credentials for the metadata repository database, follow the instructions in "Upgrading the Metadata Repository Container" on page 1-4.
- If you have administrative credentials for the Oracle Internet Directory, follow the instructions in "Upgrading the Metadata Repository Container" on page 1-4.
- If you have DBA credentials for the metadata repository database and administrative credentials for the Oracle Internet Directory, and want to perform both upgrade functions, follow the instructions in "Executing mrc.pl for New Schema Creation and Oracle Internet Directory Entry Update" on page 1-5.

Removing Invalid Packages From the Database

Before executing the `mrc.pl` script, you must check for and remove any invalid packages for default schemas from the database.

1. Check for invalid packages by running the following commands.

```
sqlplus '/as sysdba'
sql> select package_name from dba_objects where status='INVALID';
```

2. If any rows are returned, run the following commands from the new infrastructure *ORACLE_HOME*:

```
sql> @?/rdbms/admin/utlrp
```

3. Repeat until there are no invalid packages for default schemas.

Executing mrc.pl for New Schema Creation and Oracle Internet Directory Entry Update

> **Caution:** Before executing the `mrc.pl` script, you must check for and remove any invalid packages for default schemas from the database. See "Removing Invalid Packages From the Database" on page 1-5.

This method of executing `mrc.pl` combines the `d` and `u` options in one procedure. You should not perform this combined procedure if you have run `mrc.pl` with either the `d` option or the `u` option (as described in "Upgrading the Metadata Repository Container" on page 1-4 and "Upgrading the Metadata Repository Container" on page 1-4). Follow these steps to create new schemas in the metadata repository and update the Oracle Internet Directory entry:

1. Ensure that the database, listener, and Oracle Internet Directory server are running.
2. Ensure that the ORACLE_HOME environment variable is set to <*Infra_OH*> and the ORACLE_SID environment variable is set to the Infrastructure database SID. If they are not, follow the instructions in Section , "Setting the Environment for Upgrading the Metadata Repository" on page 1-3.
3. Change directories to <*repCA_CD*>`/repCA/mrc/upgrade`.
4. Ensure that there is an existing directory with write permission enabled in which to create new database files for the new tablespaces. (You will specify this directory as part of the command to start the script.)
5. Issue this command:

```
<Infra_OH>/perl/bin/perl mrc.pl du -dbpwd <SYS user
password> -dspace <tablespace directory> -ousr <oid admin
user name> -opwd <oid admin user password> -connstring
<database connect string>
```

where:

- <SYS user password> is the dba password
- <tablespace directory> is an existing directory in which you want the files that contain the new tablespaces to be created
- <oid admin user name> is the Oracle Internet Directory administrative user name
- <oid admin password> is the Oracle Internet Directory administrative user password
- <conn string> is the database connect string in the format host:port:SID

Resolving Errors

Errors may occur during the upgrade process. Common errors returned by the upgrade script and their resolution are listed below.

java.sql.SQLException: ORA-01034 ORACLE not available.

Cause: The database is not running.

Action: Start the database.

java.sql.SQLException: Io exception: The Network Adapter could not establish the connection.

Cause: The listener is not running.

Action: Start the listener.

Invalid OID password.

Cause: The Oracle Internet Directory superuser password is incorrect.

Action: Provide the correct password.

Upgrading the Identity Management Services

This section explains how to upgrade Identity Management services. Before you perform the tasks in this chapter, you must perform the steps in "Preparing to Upgrade the Metadata Repository Database" on page 1-3.

The chapter consists of the following sections:

Upgrading Identity Management

Identity Management comprises Oracle Application Server Single Sign-On and Oracle Internet Directory. This section describes possible configurations for Identity Management, and explains how to upgrade it using the Oracle Universal Installer. The following topics are included:

Identity Management Configuration Overview

In Oracle9iAS Release 2 (9.0.2), a database tier is required to operate Oracle Application Server Single Sign-On and Oracle Internet Directory. The Metadata Repository contains the necessary schemas for these components.

An Oracle9iAS Release 2 (9.0.2) Identity Management configuration can be non-distributed, in which Oracle Application Server Single Sign-On and Oracle Internet Directory share a metadata repository. This is depicted in Figure 1–1. Alternatively, the Identity Management configuration can be distributed, in which Oracle Application Server Single Sign-On and Oracle Internet Directory each use a separate metadata repository. This is depicted in Figure 1–2.

In Oracle Application Server Release 2 (9.0.4), the distributed configuration is different from that in Release 2 (9.0.2), in that a single Metadata Repository is shared between Oracle Application Server Single Sign-On and Oracle Internet Directory, and Oracle Application Server Single Sign-On accesses it from a different computer. This is shown in Figure 1–3.

Notes: As shown in Figure 1–1, the non-distributed configuration in the Release 2 (9.0.4) release is similar to that in Oracle9*i*AS Release 2 (9.0.2)

If, in Oracle9iAS Release 2 (9.0.2), you had a Delegated Administration Services (DAS) or Directory Integration and Provisioning (DIP) operating in a middle tier, and you want to set up a DAS or DIP in Release 2 (9.0.4), you must perform a DAS-only or DIP-only installation in a separate Oracle home. See the section titled "Installing Identity Management Components Only" in the chapter "Installing OracleAS Infrastructure 10*g*" in the *Oracle Application Server 10g Installation Guide*.

Figure 1–1 Non-Distributed Identity Management in Release 2 (9.0.2) and Release 2 (9.0.4)

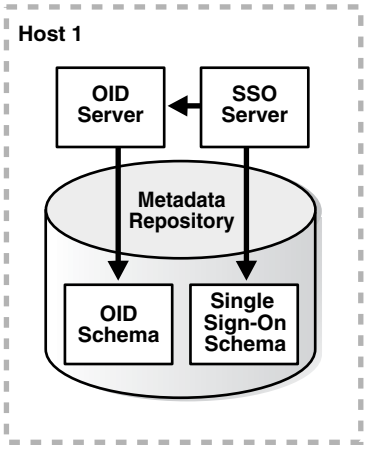


Figure 1–2 Distributed Identity Management in Release 2 (9.0.2)

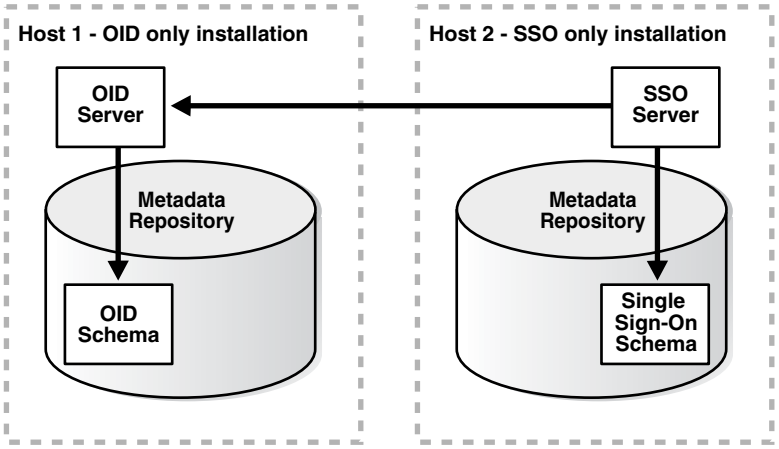
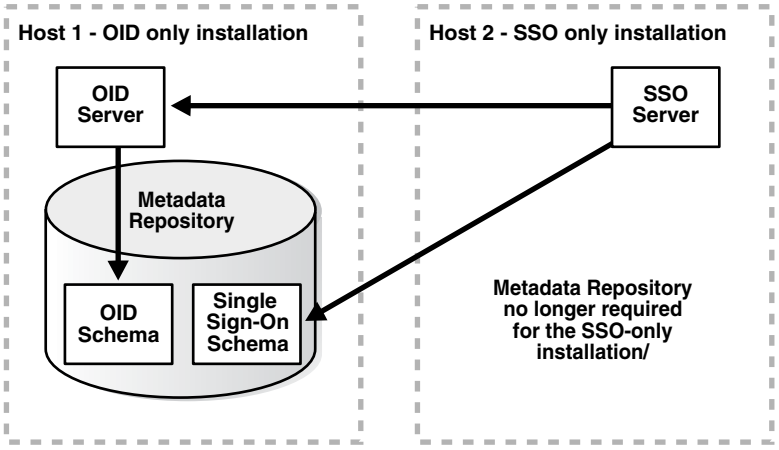


Figure 1–3 Distributed Identity Management in Release 2 (9.0.4)

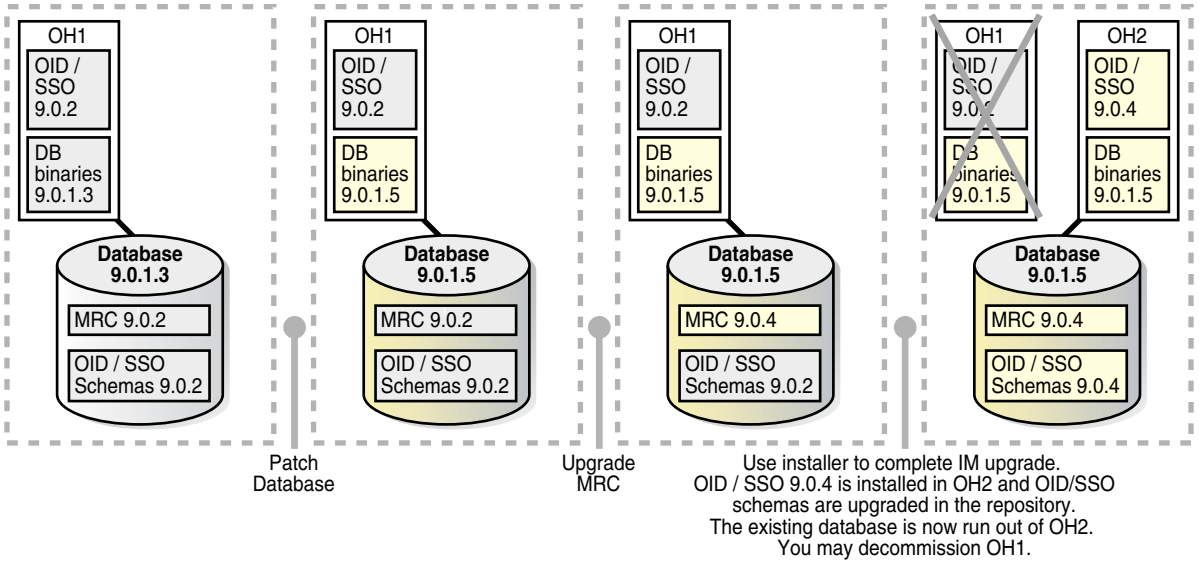


Understanding the Identity Management Upgrade Processes

The Identity Management schemas are contained in the Metadata Repository, along with other component schemas (such as those for OracleAS Portal and Oracle Ultra

Search). However, the upgrade process for the Identity Management schemas (labeled OID/SSO in Figure 1–4) is different from the upgrade process for the component schemas (labeled MRC in Figure 1–4). The Identity Management schemas are upgraded by the Oracle Universal Installer, as shown in Figure 1–4, "Identity Management Upgrade". The component schemas are upgraded by individual scripts.

Figure 1–4 Identity Management Upgrade



The Identity Management Upgrade Process

> **Note:** Before the Identity Management services can be upgraded, the 9.0.1.5 patch must be applied to the database.

The Identity Management upgrade consists of these steps:

1. The Metadata Repository Container Upgrade script is run.

   > **Note:** The Metadata Repository Container Upgrade script upgrades the Metadata Repository that is in use by the Identity Management services being upgraded. After this script is run, no new Oracle9*i*AS Release 2 (9.0.2) middle tier installations may use this Metadata Repository. However, existing Oracle9*i*AS Release 2 (9.0.2) middle tier installations will continue to function.

2. The Oracle Universal Installer is started; Oracle Internet Directory and Oracle Application Server Single Sign-On are installed in the new Oracle home and Oracle Internet Directory and Oracle Application Server Single Sign-On schemas are upgraded in the Metadata Repository.
3. All post-upgrade steps that are applicable to the upgraded configuration are performed, as described in "Performing Infrastructure Post-Upgrade Tasks" on page 1-35.

Note: Do not manually delete any database (`*.dbf`) files that remain in the Oracle9*i*AS Release 2 (9.0.2) Infrastructure Oracle home (labeled OH1 in Figure 1–4) after Identity Management is upgraded to Oracle Application Server Release 2 (9.0.4). The Identity Management upgrade process does not copy or relocate any (`*.dbf`) files or redo log files to the destination Oracle home. If the (`*.dbf`) files were located in the source Oracle home before the Identity Management upgrade, they will remain there after the upgrade, unless you relocate them. For information on relocating the database files to the destination Oracle home, see "Decommissioning the Release 2 (9.0.2) Oracle Home" on page 1-44.

Using Oracle Universal Installer to Upgrade Identity Management

The Identity Management upgrade is performed by Oracle Universal Installer. Oracle Universal Installer launches configuration assistants that upgrade the Oracle Internet Directory and Oracle Application Server Single Sign-On database schema. This upgrade can only be performed by a user with `SYS` credentials.

Before you start the Identity Management upgrade, ensure that:

- The steps in "Preparing to Upgrade the Metadata Repository Database" on page 1-3 have been performed.
- The database server is running.
- The database listener is running.
- The Oracle Internet Directory server is running. To verify this, issue the following commands (each should return `"bind successful"`):

  ```
  <source_Infra_OH>/bin/ldapbind -p <Non-SSL port>

  <source_Infra_OH>/bin/ldapbind -p <SSL port> -U 1
  ```

This section contains the following topics:

Upgrading a Non-Distributed Identity Management Configuration

Follow these steps to upgrade a non-distributed Identity Management configuration (depicted in Figure 1–1, "Non-Distributed Identity Management in Release 2 (9.0.2) and Release 2 (9.0.4)"). Oracle Universal Installer will prompt you to stop and start certain components during the upgrade.

1. Log in to the computer on which Oracle9*i*AS Release 2 (9.0.2) is installed, as the same operating system user that performed the Oracle9*i*AS Release 2 (9.0.2) installation.
2. Mount the CD-ROM.

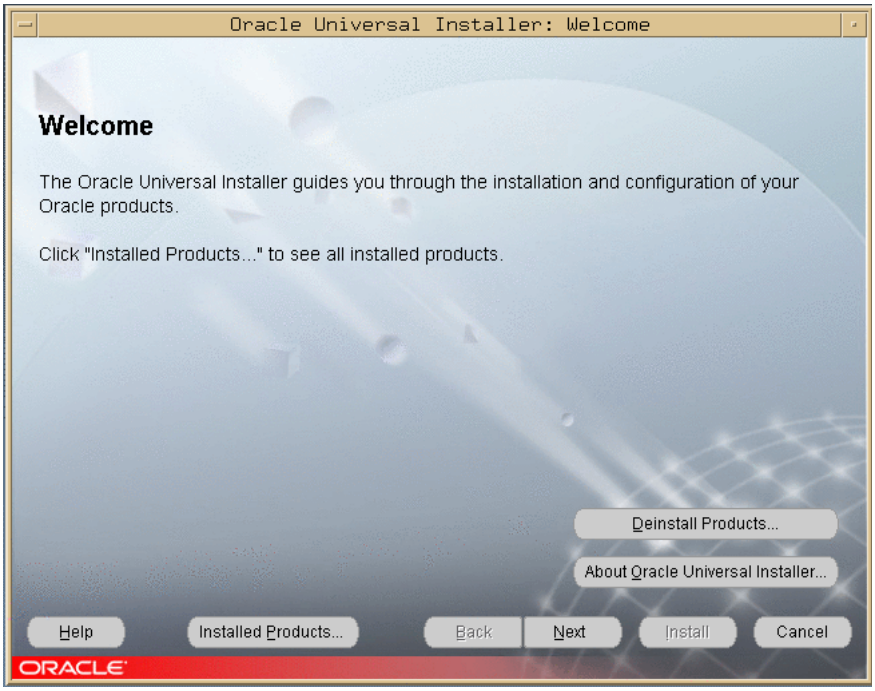
   See Also: *Oracle Application Server 10g Installation Guide*

3. Start the installer.

   See Also: *Oracle Application Server 10g Installation Guide*

   The Welcome screen appears as shown in Figure 1–5.

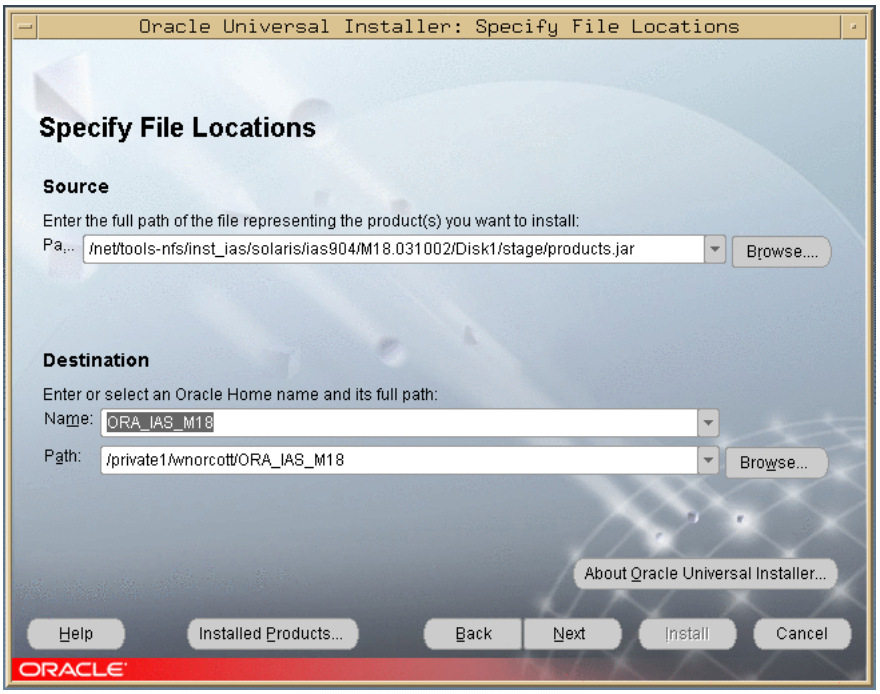
Figure 1–5 Welcome Screen



4. Click **Next**.

   The Specify File Locations screen appears as shown in Figure 1–6.

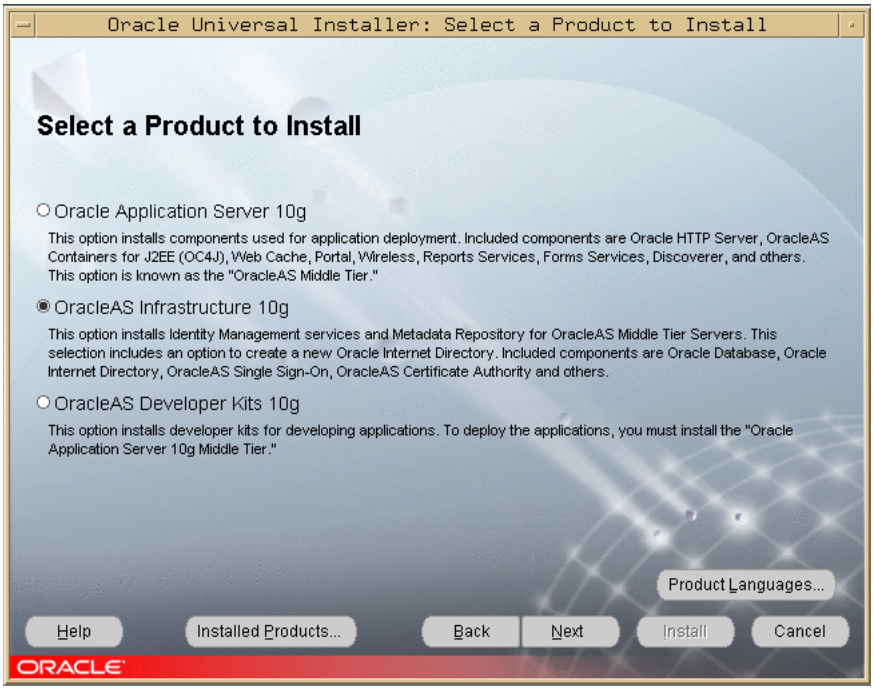
Figure 1–6 Specify File Locations Screen



5. Enter a new Oracle home name and a path for the Release 2 (9.0.4) upgrade and click **Next**.

   The Select a Product To Install screen appears as shown in Figure 1–7.

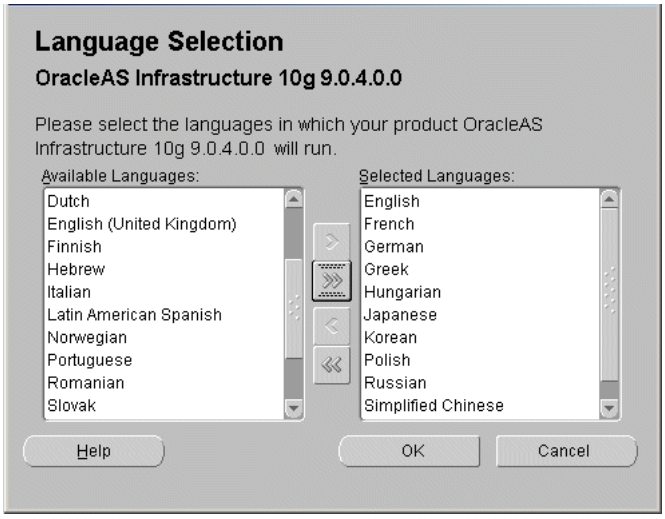
Figure 1–7 Select a Product to Install Screen



6. Select OracleAS Infrastructure 10*g*. If multiple languages are used in the Oracle9iAS Release 2 (9.0.2) Infrastructure, then click Product Languages. If you want only English to be installed in Oracle Application Server Release 2 (9.0.4), then click **Next** and continue with Step 8.

   The Language Selection screen appears as shown in Figure 1–8.

Figure 1–8 Language Selection Screen



7. Select the languages you want to install and click **OK**.

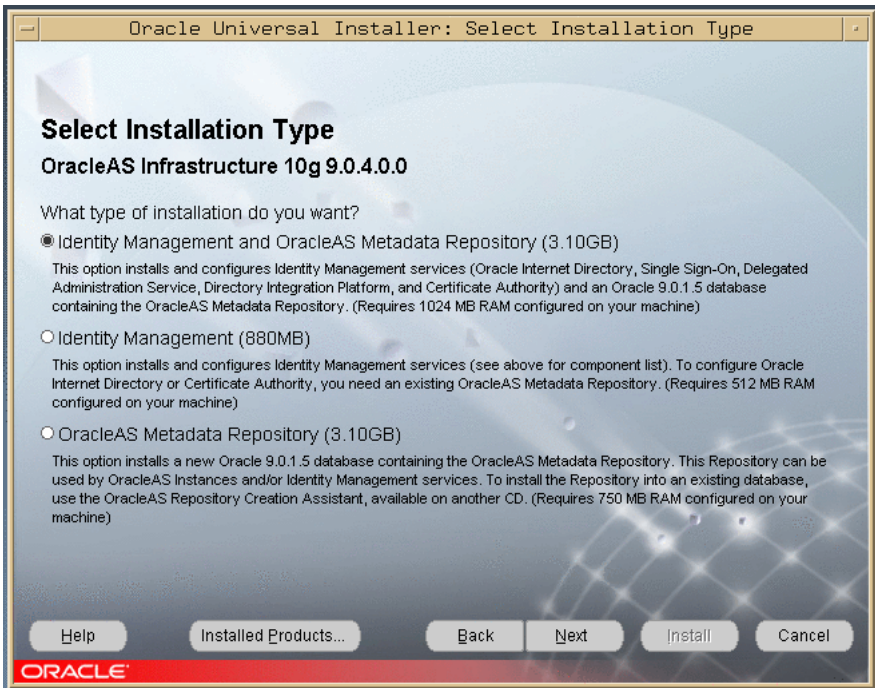
Note: If multiple languages were installed in Oracle9*i*AS Release 2 (9.0.2), select those languages. If you are not sure which languages were installed, but want languages other than English, click the double arrow button (>>) to select all languages.

The Select a Product to Install screen appears again.

8. Click Next.

   The Select Installation Type screen appears as shown in Figure 1–9.

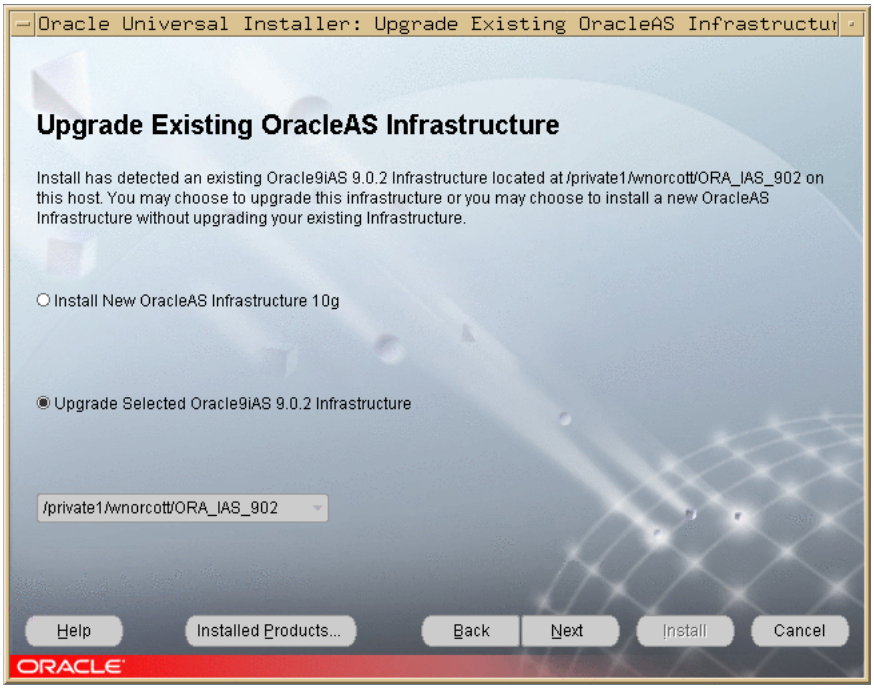
Figure 1–9 Select Installation Type Screen



9. Select Identity Management and OracleAS Metadata Repository and click **Next**.

   The Upgrade Existing Infrastructure screen appears as shown in Figure 1–10.

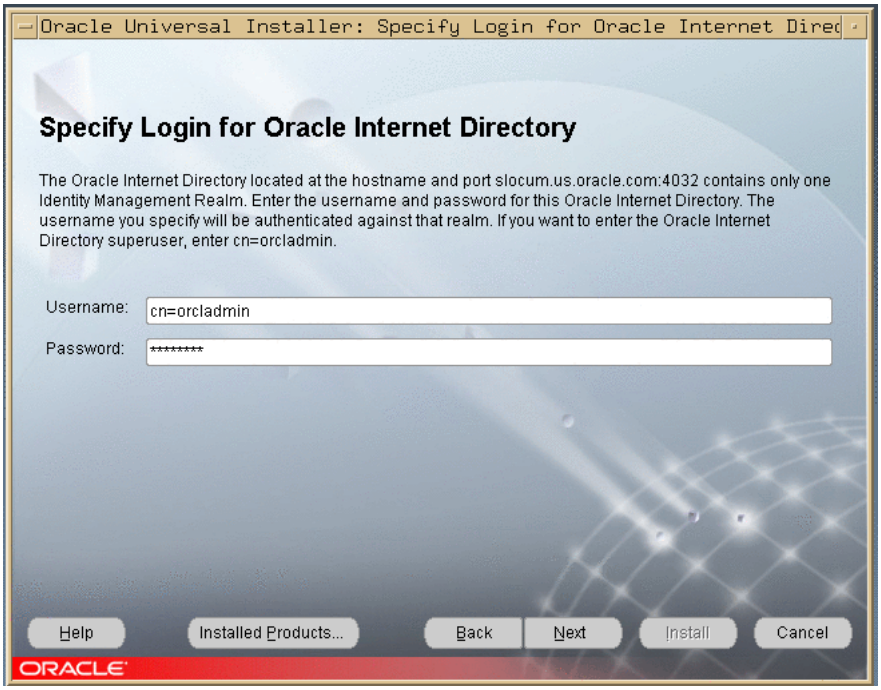
Figure 1–10 Upgrade Existing OracleAS Infrastructure Screen



10. Select Upgrade Selected Oracle9*i*AS 9.0.2 Infrastructure.
11. Select the Infrastructure you want to upgrade from the drop-down list, then click **Next**. (If there is only one Infrastructure on the computer, then the drop-down list is inactive.)

    The Specify Login for Oracle Internet Directory screen appears as shown in Figure Figure 1–11.

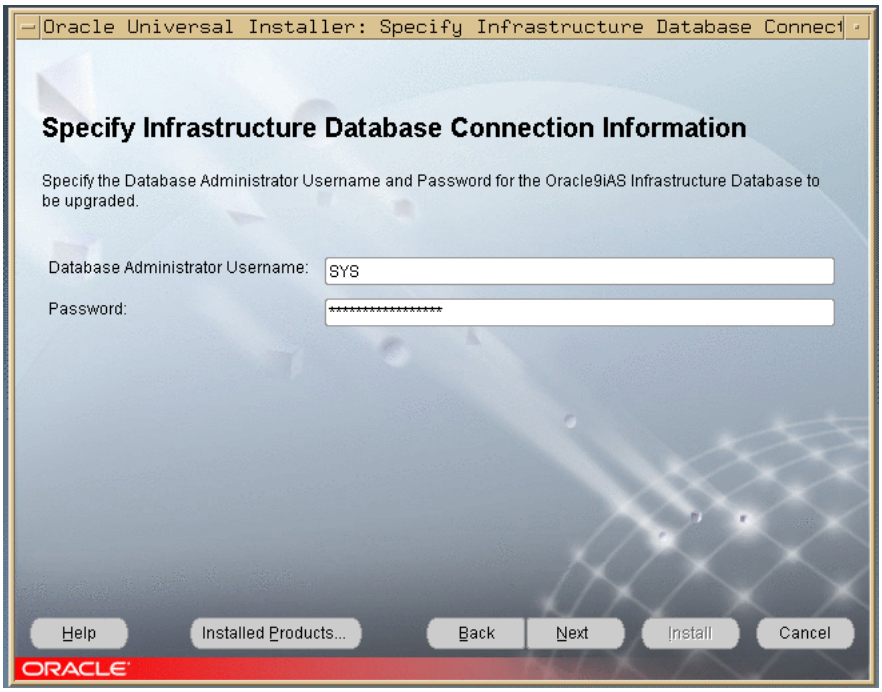
Figure 1–11 Specify Login for Oracle Internet Directory Screen



12. Enter the OID superuser DN in the **Username** field. The superuser DN `cn=orcladmin` is the default for this field; change this value if the OID superuser DN is not `cn=orcladmin`.
13. Enter the password in the Password field and click **Next**.

    The Specify Infrastructure Database Connection screen appears as shown in Figure 1–27.

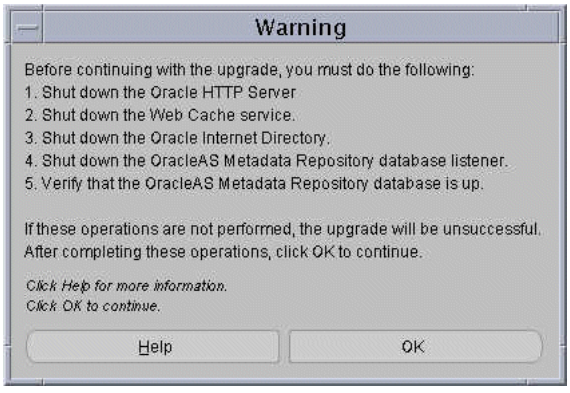
Figure 1–12 Specify Infrastructure Database Connection Information Screen



14. Enter `SYS` in the **Username** field and the `SYS` user's password in the **Password** field and click **Next**.

    A warning dialog appears as shown in Figure 1–13, instructing you to stop processes in the Oracle home.

Figure 1–13 Warning Dialog

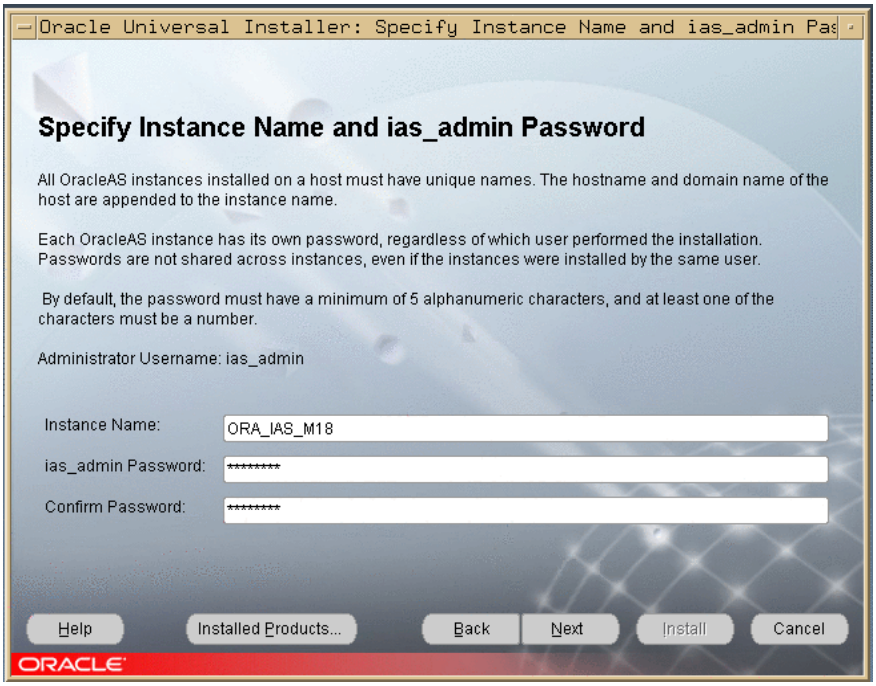


15. Stop Oracle Internet Directory and the Metadata Repository database listener.
16. Stop all processes in the Oracle home.

17. Ensure that the Metadata Repository database is running, then click **OK**.

    The Specify Instance Name and ias_admin Password screen appears as shown in Figure 1–14.

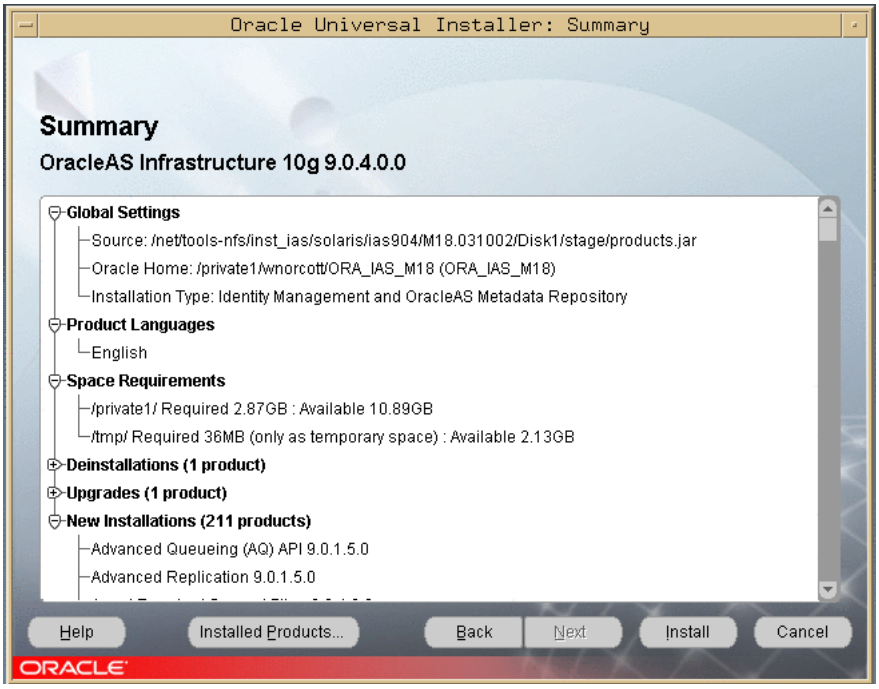
Figure 1–14 Specify Instance Name and ias_admin Password Screen



18. Complete the **Instance Name**, **ias_admin Password**, and **Confirm Password** fields and click **Next**.

    The Summary screen appears as shown in Figure 1–15.

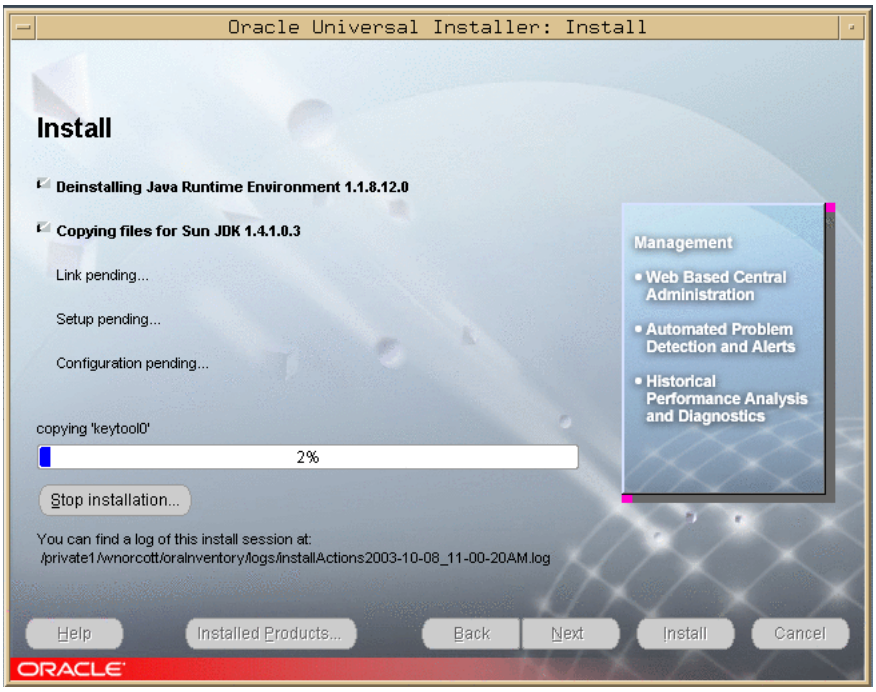
Figure 1–15 Summary Screen



19. Click Install.

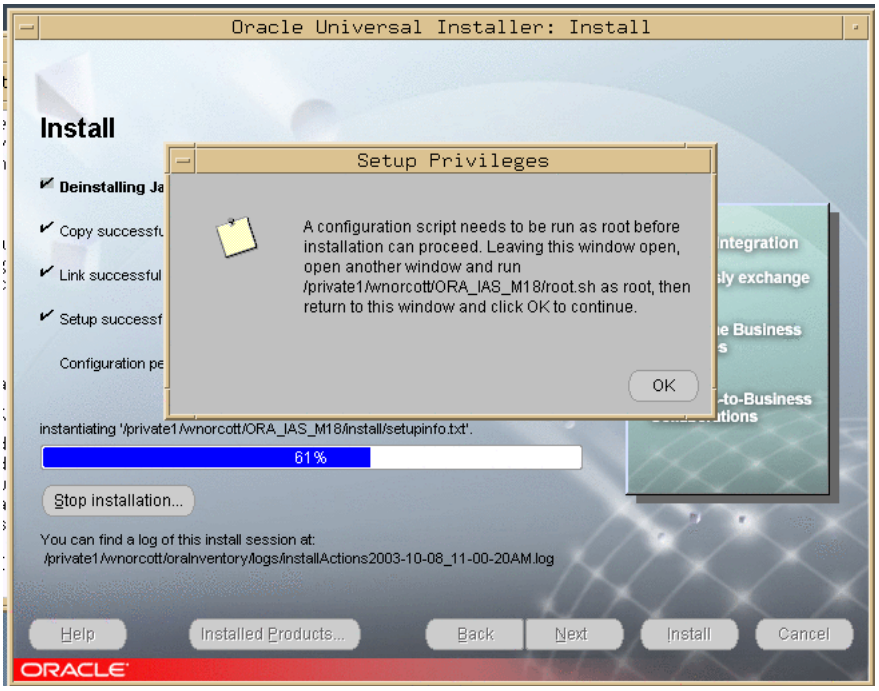
The Install screen appears as shown in Figure 1–16, and the upgrade starts. The processing time varies, but it will be several minutes before you are prompted to take any action.

Figure 1–16 Install Screen



The Setup Privileges dialog appears as shown in Figure 1–17.

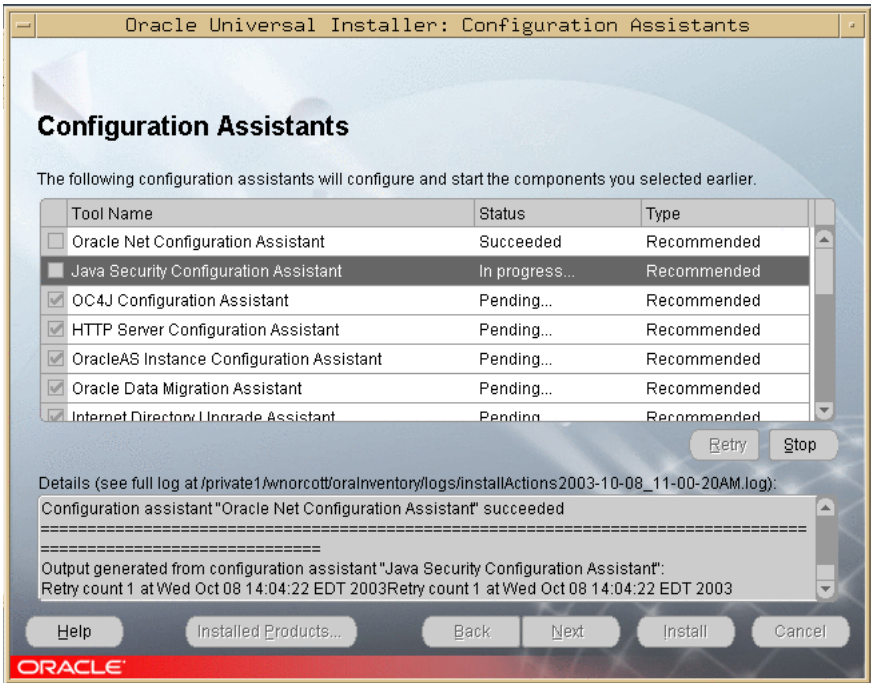
Figure 1–17 Install Screen and Setup Privileges Dialog



20. Open a window and run the script, then click **OK** in the dialog.

The script may take a few minutes to complete, depending on the speed and workload of the computer on which it is running. After the script completes, the Configuration Assistants screen appears as shown in Figure 1–18. The configuration process is lengthy.

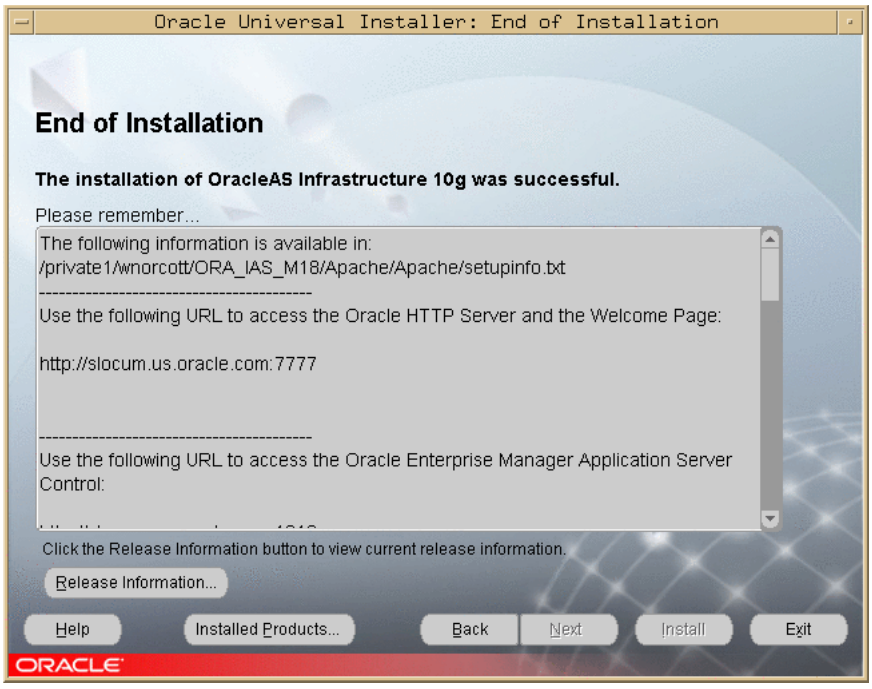
Figure 1–18 Configuration Assistants Screen



21. Click **Next**.

After several minutes, the End of Installation screen appears as shown in Figure 1–19.

Figure 1–19 End of Installation Screen



22. Verify that Oracle Internet Directory and Oracle Application Server Single Sign-On are functioning and accessible.

> **See Also:** *Oracle Application Server 10g Administrator's Guide*, Chapter 1, "Accessing the Single Sign-On Server".

Upgrading a Distributed Identity Management Configuration

Follow the steps below to upgrade a distributed Identity Management configuration (depicted in Figure 1–2, "Distributed Identity Management in Release 2 (9.0.2)").This upgrade includes separate processes for Oracle Internet Directory and OracleAS Single Sign-On.

Performing the Oracle Internet Directory Upgrade Perform the steps in "Using Oracle Universal Installer to Upgrade Identity Management" on page 1-10, and "Upgrading a Non-Distributed Identity Management Configuration" on page 1-10.

After the upgrade, the Oracle Internet Directory server is running in the new Oracle home.

> **Note:** The Release 2 (9.0.2) installation of Oracle Application Server Single Sign-On is still functional after the Oracle Internet Directory upgrade. In general, however, the operation of middle tiers that are installed, upgraded, or re-configured to run with partially upgraded Identity Management Services is not supported.

Performing the Oracle Application Server Single Sign-On Upgrade Perform the steps below to upgrade the Oracle Application Server Single Sign-On server. Before you begin, ensure that:

- The Oracle Internet Directory upgrade is complete.
- You have credentials for the Oracle Application Server Single Sign-On database.
- You have credentials for the Oracle Internet Directory database.
- The Oracle Internet Directory database is running.

1. Log in to the computer on which Oracle9*i*AS Release 2 (9.0.2) Oracle Application Server Single Sign-On is installed.
2. Mount the CD-ROM.

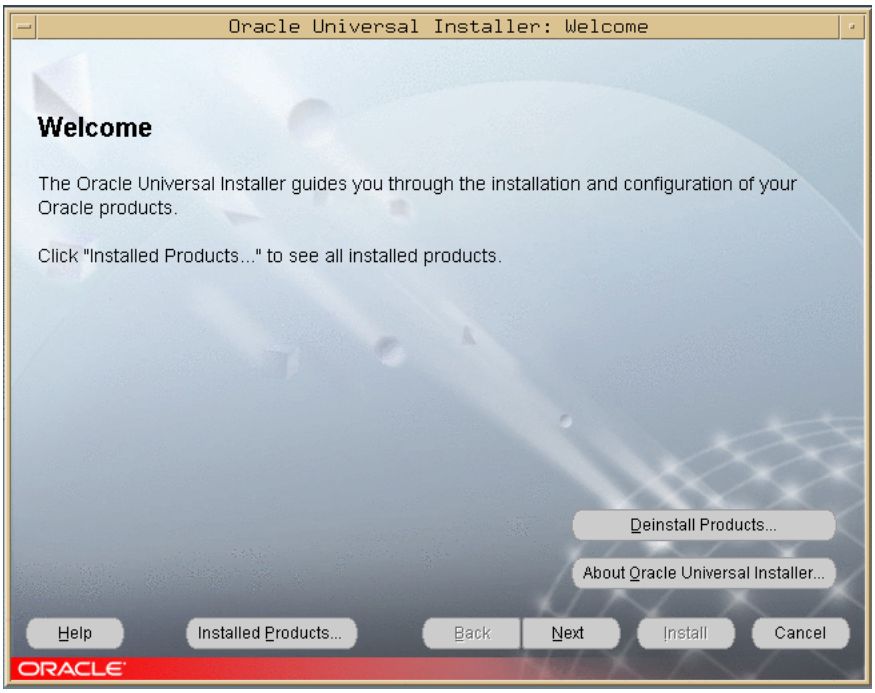
   See Also: *Oracle Application Server 10g Installation Guide*

3. Start the installer.

   See Also: *Oracle Application Server 10g Installation Guide*

   The Welcome screen appears as shown in Figure 1–20.

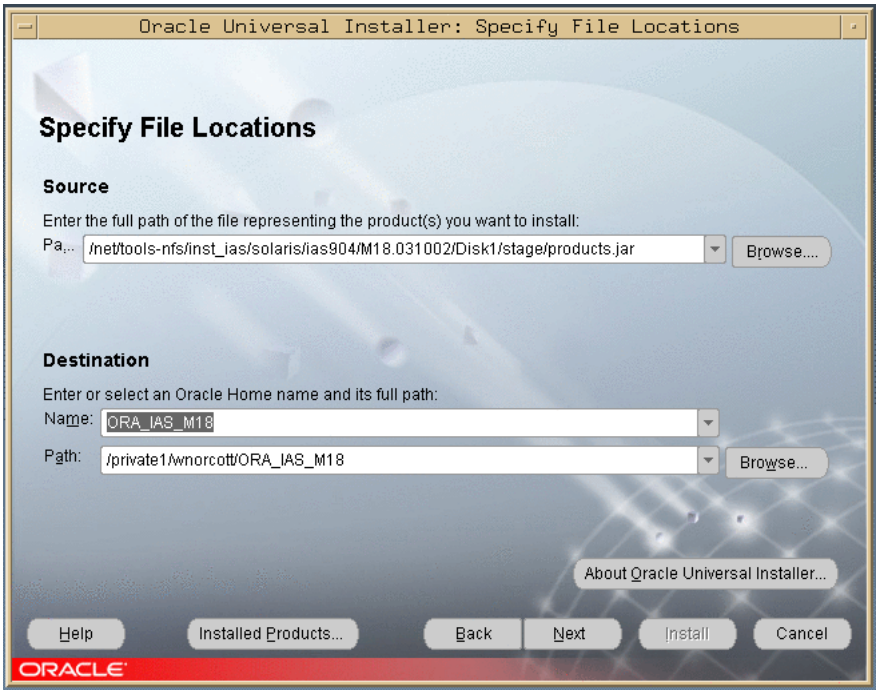
Figure 1–20 Welcome Screen



4. Click **Next**.

   The Specify File Locations screen appears as shown in Figure 1–21.

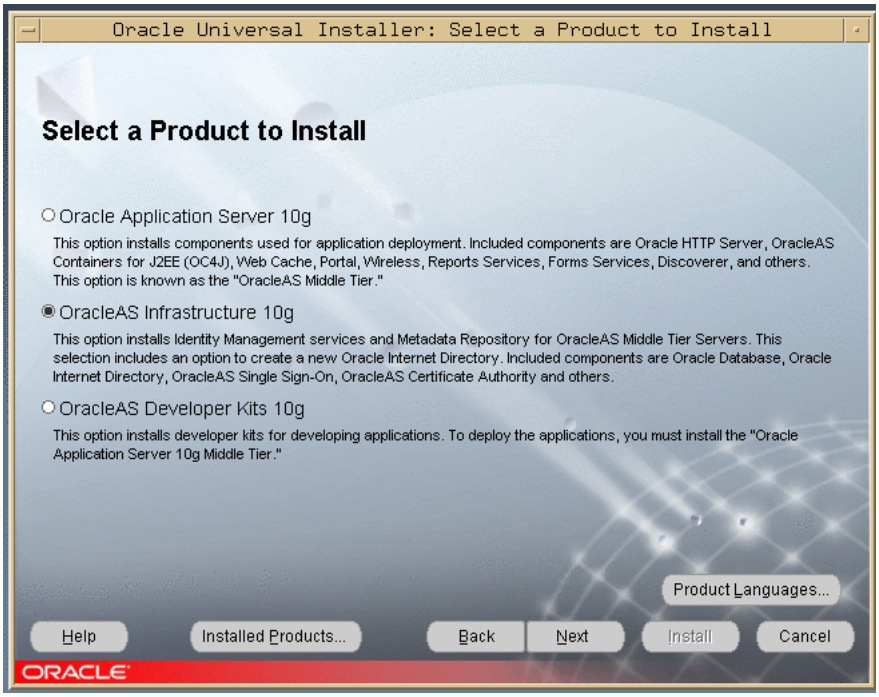
Figure 1–21 Specify File Locations Screen



5. Enter a new Oracle home name and path for the Release 2 (9.0.4) upgrade and click **Next**.

   The Select a Product To Install screen appears as shown in Figure 1–22.

Figure 1–22 Select a Product to Install Screen

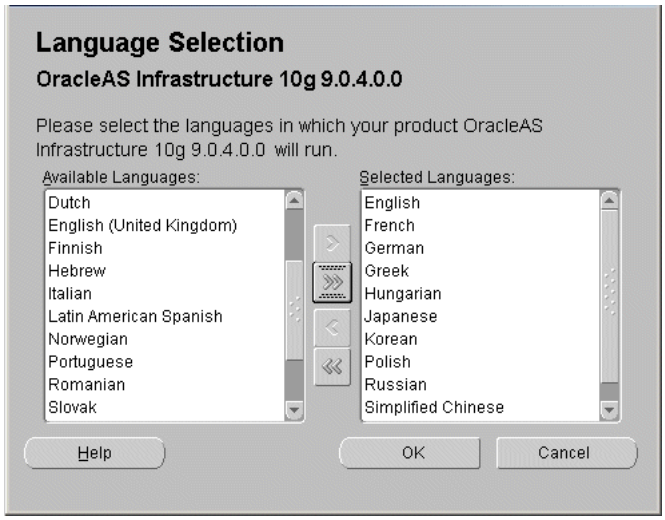


6. Select OracleAS Infrastructure 10*g*. If multiple languages are used in the Oracle9iAS Release 2 (9.0.2) Infrastructure, then click **Product Languages**. If you

want only English to be installed in Oracle Application Server Release 2 (9.0.4), then click **Next** and continue with Step 8.

The Language Selection screen appears as shown in Figure 1–23.

Figure 1–23 Language Selection Screen



7. Select the languages you want and click **OK**.

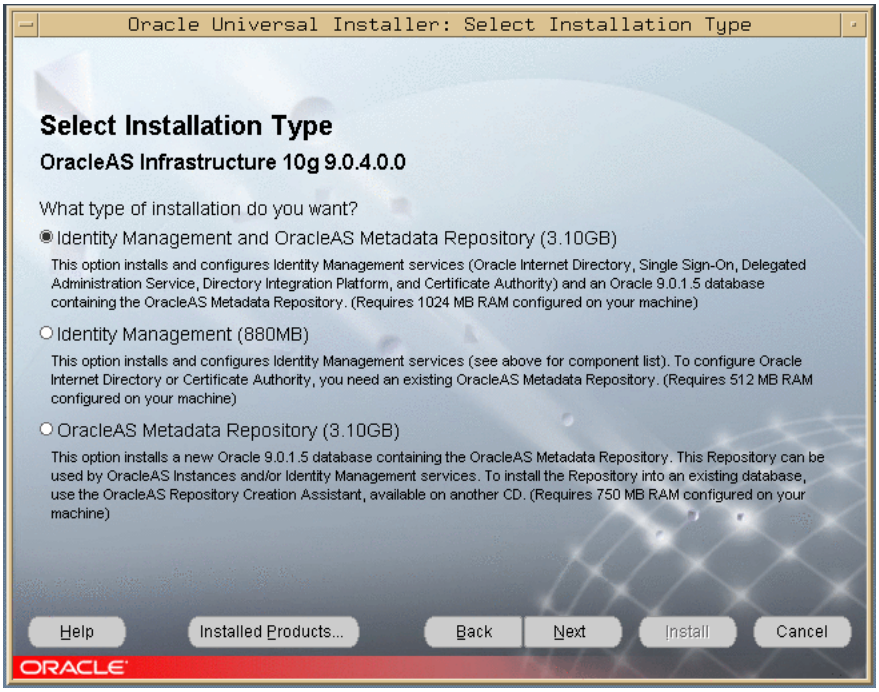
> **Note:** If multiple languages were installed in Oracle9*i*AS Release 2 (9.0.2), select those languages. If you are not sure which languages were installed, but want languages other than English, click the double arrow button (>>) to select all languages.

The Select a Product To Install screen appears again.

8. Click **Next**.

The Select Installation Type screen appears as shown in Figure 1–24.

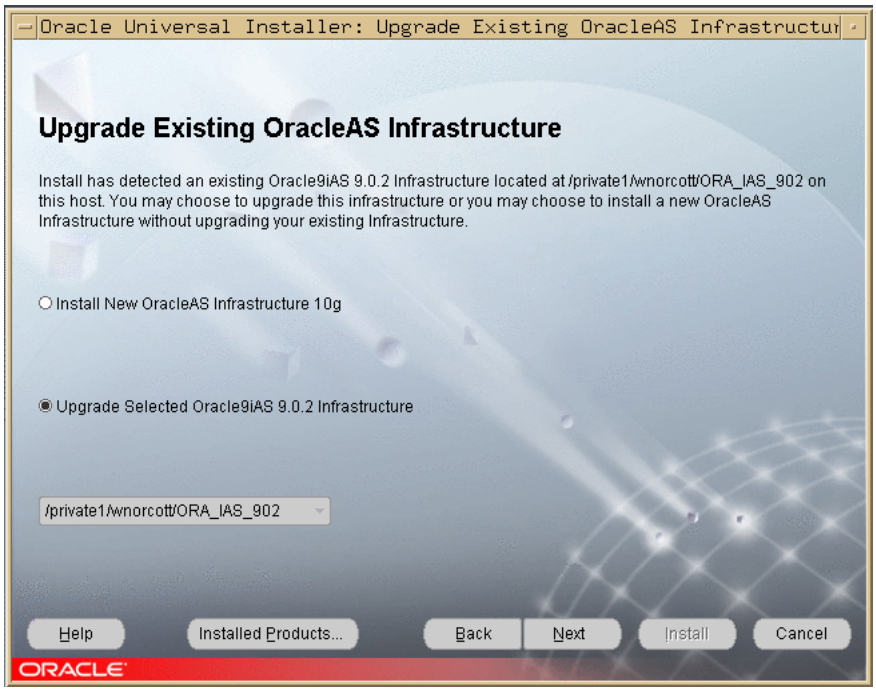
Figure 1–24 Select Installation Type Screen



9. Select Identity Management and OracleAS Metadata Repository and click **Next**.

   The Upgrade Existing Infrastructure screen appears as shown in Figure 1–25.

Figure 1–25 Upgrade Existing OracleAS Infrastructure Screen

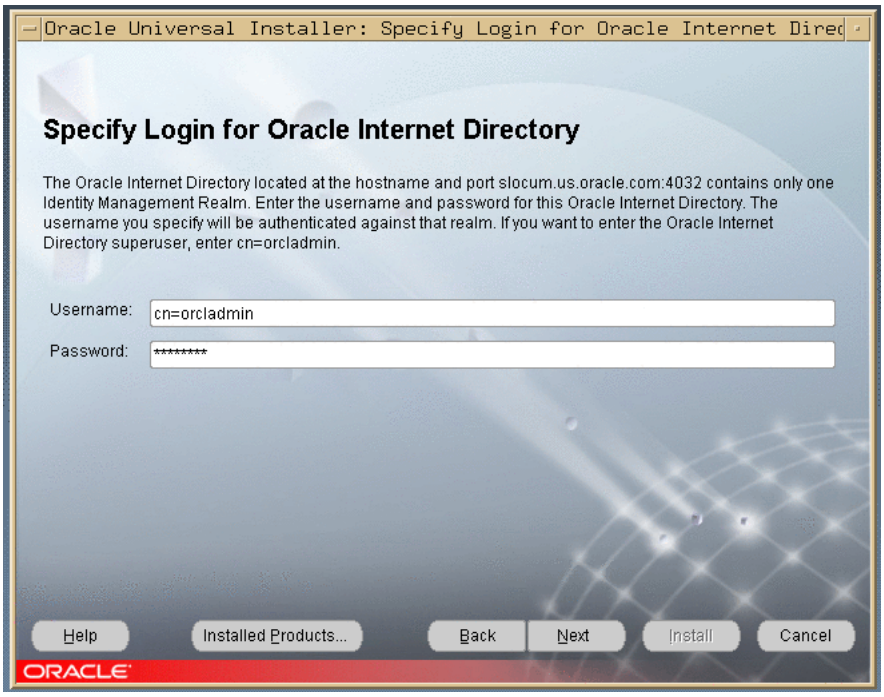


10. Ensure that the database listener in the Oracle9*i*AS Release 2 (9.0.2) Oracle Application Server Single Sign-On Oracle home is running.
11. Select Upgrade Selected Oracle9*i*AS 9.0.2 Infrastructure.

12. Select the Infrastructure you want to upgrade from the drop-down list, then click Next. (If there is only one Infrastructure, the drop-down list is inactive.)

    The Specify Login for Oracle Internet Directory screen appears as shown in Figure Figure 1–26.

Figure 1–26 Specify Login for Oracle Internet Directory Screen

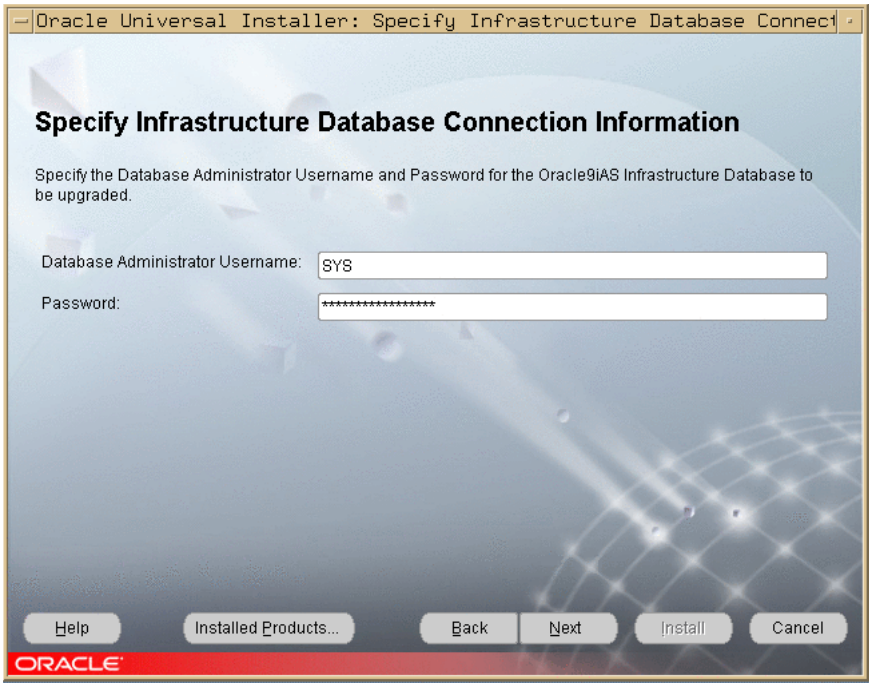


13. Enter the Oracle Internet Directory superuser DN in the **Username** field. The superuser DN **cn=orcladmin** is the default for this field; change this value if the DN is not cn=orcladmin.

14. Enter the password in the Password field and click Next.

    The Specify Infrastructure Database Connection screen appears as shown in Figure 1–27.

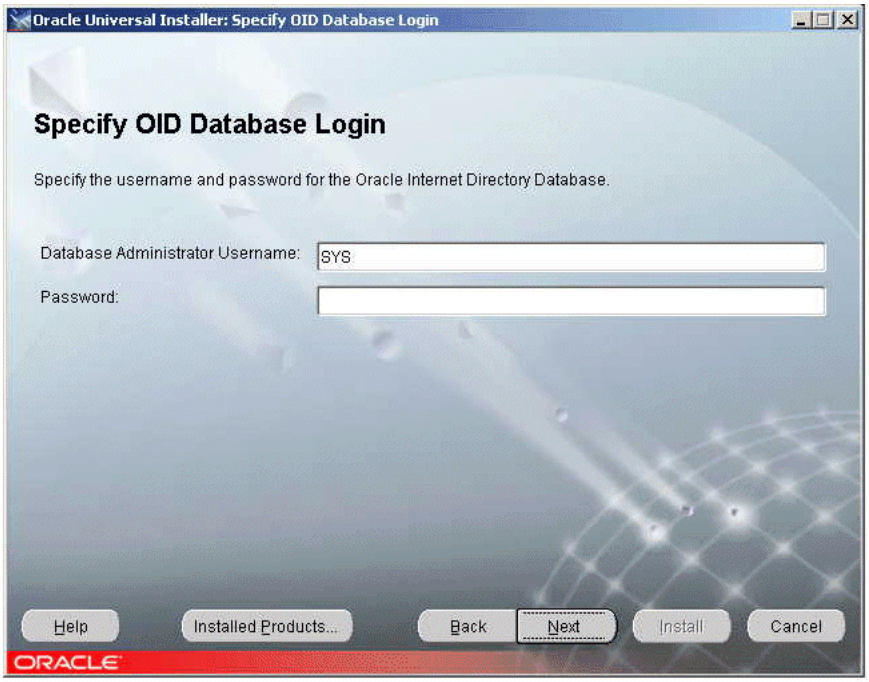
Figure 1–27 Specify Infrastructure Database Connection Information Screen



15. Enter the Oracle Application Server Single Sign-On SYS user name in the **Username** field and the `SYS` user's password in the Password field and click **Next**. You are connecting to the Oracle Application Server Single Sign-On database.

    The Specify OID Database Login screen appears as shown in Figure 1–28.

Figure 1–28 Specify OID Database Login Screen



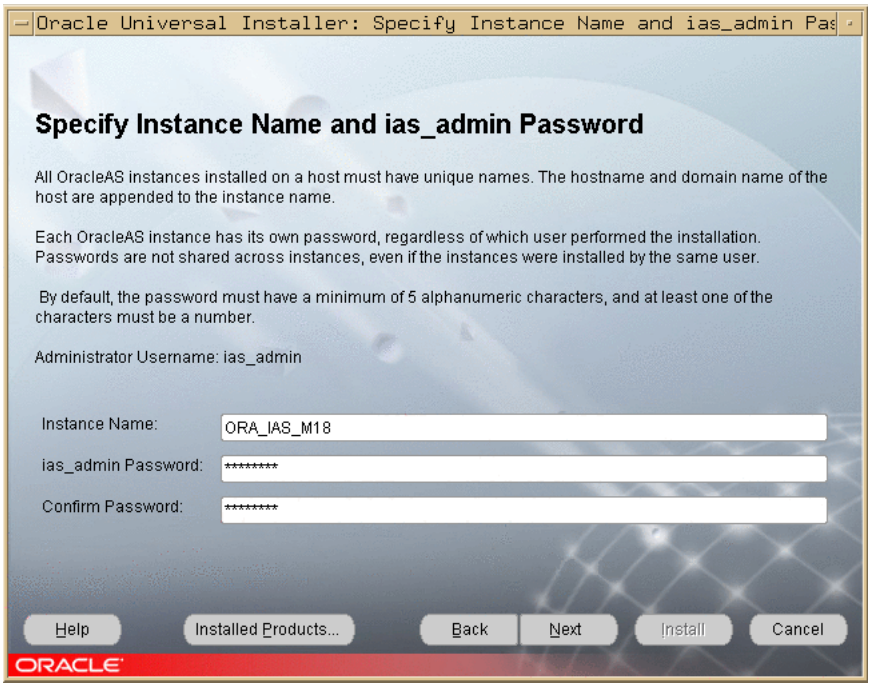
16. Enter the Oracle Internet Directory Database `SYS` user name in the Database Administrator **Username** field and the password in the password field, then click **Next**.

    A warning dialog appears, instructing you to stop processes in the Oracle home.

17. Stop the Oracle HTTP Server and click **OK**.

    The Specify Instance Name and ias_admin Password screen appears as shown in Figure 1–29.

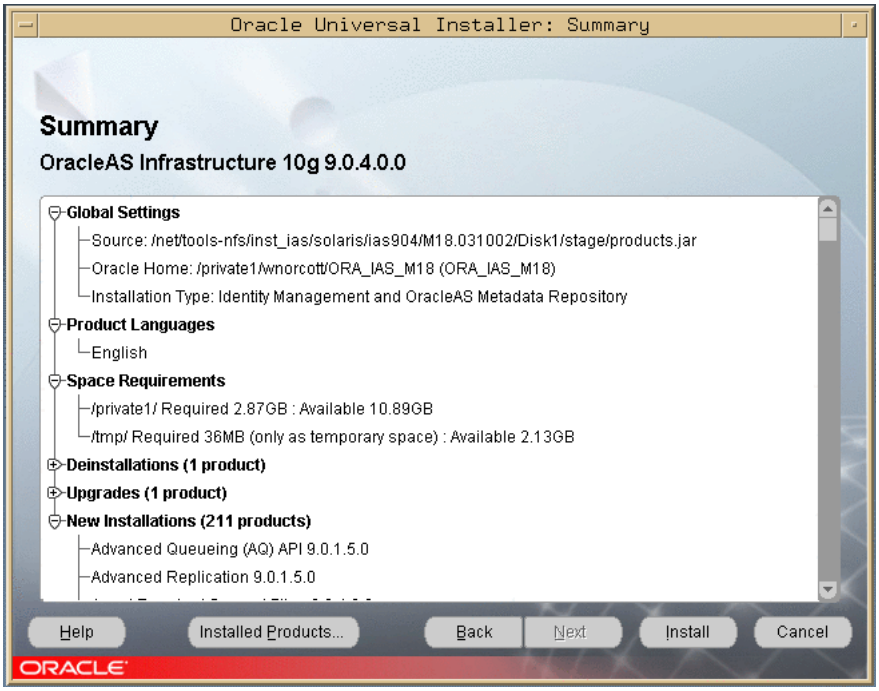
Figure 1–29 Specify Instance Name and ias_admin Password Screen



18. Complete the **Instance Name**, **ias_admin Password**, and **Confirm Password** fields and click **Next**.

    The Summary screen appears as shown in Figure 1–30.

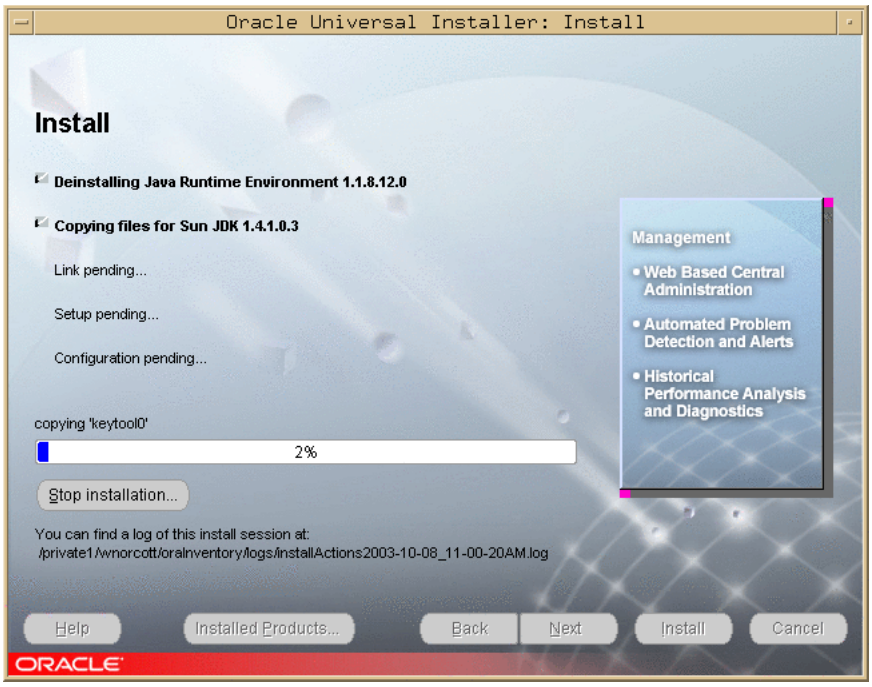
Figure 1–30 Summary Screen



19. Click **Install**.

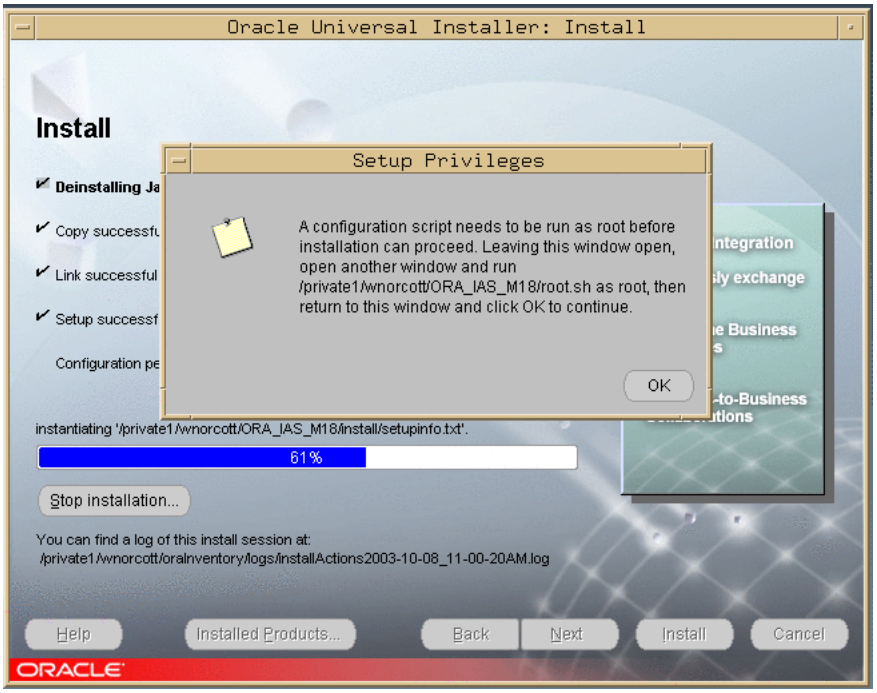
The Install screen appears as shown in Figure 1–31, and the upgrade starts. The processing time varies, but it will be several minutes before you are prompted to take any action.

Figure 1–31 Install Screen



The Setup Privileges dialog appears as shown in Figure 1–32.

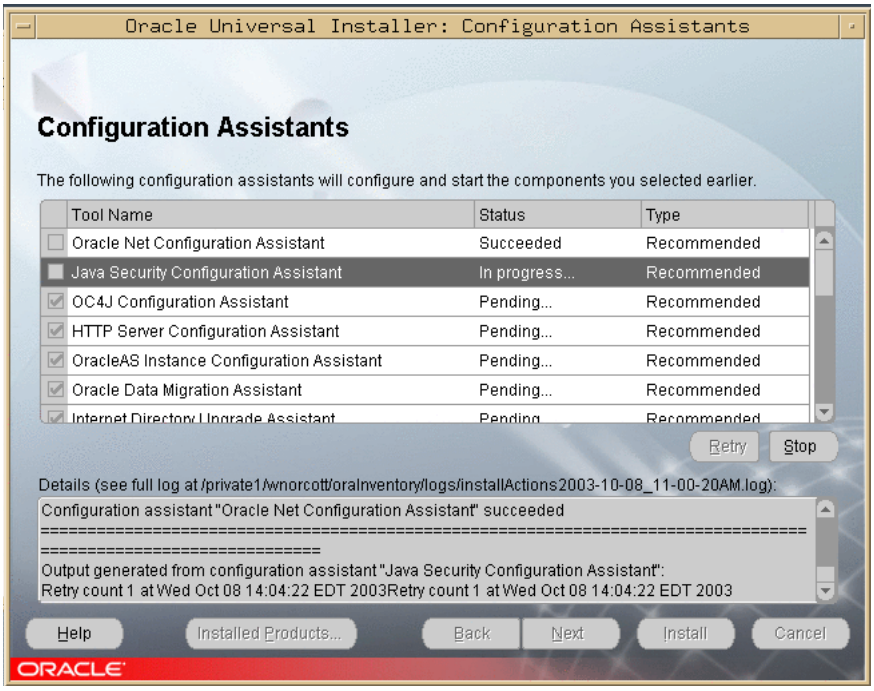
Figure 1–32 Install Screen and Setup Privileges Dialog



20. Open a window and run the script, then click **OK** in the dialog.

The script may take up to an hour to complete, depending on the speed and workload of the computer on which it is running. After the script completes, the Configuration Assistants screen appears as shown in Figure 1–33. The configuration process is lengthy.

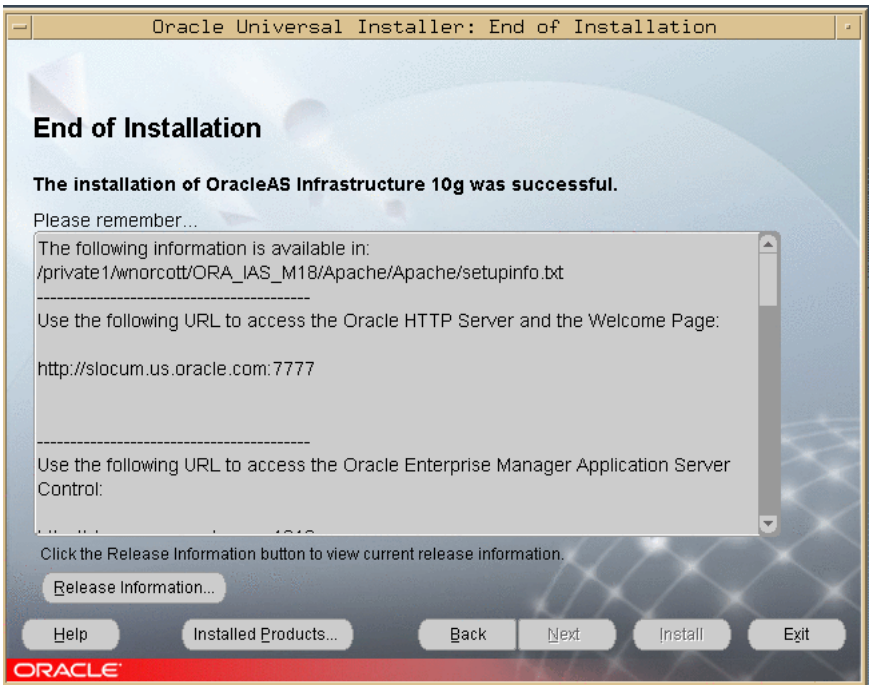
Figure 1–33 Configuration Assistants Screen



21. Click **Next**.

The End of Installation screen appears as shown in Figure 1–34.

Figure 1–34 End of Installation Screen



Note: If the Delegated Administration Services was running in the Oracle9*i*AS Release 2 (9.0.2) Oracle Internet Directory or OracleAS Single Sign-On Oracle home, and you wish to configure it in the Oracle Application Server Release 2 (9.0.4) Oracle Internet Directory or OracleAS Single Sign-On Oracle home, you can do this using the Oracle Enterprise Manager Application Server Control. For instructions, see "Configuring Oracle Delegated Administration Services by Using Oracle Enterprise Manager Application Server Control" in the *Oracle Internet Directory Administrator's Guide*.

22. Verify that Oracle Application Server Single Sign-On is functioning and accessible.

See Also: *Oracle Application Server 10g Administrator's Guide*, Chapter 1, "Accessing the Single Sign-On Server".

Performing an Oracle Internet Directory Multi-Master Replication Upgrade

This section describes how to upgrade Oracle Internet Directory in a replicated environment. You can upgrade one computer at a time, or all of the computers at one time. Instructions are provided for each method in the following sub-sections:

- "Upgrading Oracle Internet Directory on One Replica" on page 1-30
- "Upgrading Oracle Internet Directory on Multiple Replicas Simultaneously" on page 1-32

Oracle Corporation recommends that during upgrade, in order to prevent conflicts, the replication environment be a Single Master (that is, only one replica is read/write and all others are read only).

Upgrading Oracle Internet Directory on One Replica

Upgrading one computer at a time makes Oracle Internet Directory available during the upgrade for additions, modifications, and searching.

Follow these steps to upgrade one replica at a time:

1. Identify and upgrade the Master Definition Site (MDS).

   See Also: *Oracle Internet Directory Administrator's Guide*, Chapter 25, Managing Directory Replication

2. Stop the replication server, the LDAP server, and `oidmon` on the replica to be upgraded.
3. Delete all Advanced Symmetric Replication (ASR) jobs on other replicas in the replicated environment by issuing the command:

   `<source_Infra_OH>/ldap/admin/delasrjobs.sql`

   All ASR jobs on other master sites that transfer changes to the MDS are deleted. This has the effect of taking the MDS out of the replication environment, so that no changes come to it, while other replicas continue to operate and replicate changes.
4. Stop the database and listener on the replica to be upgraded.
5. Start the Oracle Universal Installer.

   The database and Oracle Internet Directory are upgraded.
6. Start the database and the listener.
7. Test the connectivity to other replicas. The Net8 migration assistant might have modified `listener.ora` and `tnsnames.ora`, breaking connectivity. If connectivity is broken, identify the entries that were modified in the files, and restore the entries from the files in *<source_Infra_OH>*`/network/admin/` to the corresponding files:

   <destination_Infra_OH>`/network/admin/listener.ora`

   <destination_Infra_OH>`/network/admin/sqlnet.ora`

   See Section 3.8.5.3, "Upgrading the tnsnames.ora File" on page 3-60 for instructions and cautions on modifying the `tnsnames.ora` file.
8. Create jobs on each replica, after it is upgraded, by issuing the command:

   `<destination_Infra_OH>/ldap/admin/remtool -asrrectify`

   The jobs that were deleted in Step 3 are re-created. They will begin transferring the existing changes and new changes from other replicas to the upgraded replicas.
9. Perform the post-upgrade procedures.

   See Also: "Completing the Oracle Internet Directory Upgrade" on page 1-36.

10. After upgrading the Infrastructure to Oracle Application Server Release 2 (9.0.4), include the ORACLE_SID environment variable in the *<destination_Infra_OH>*`/opmn/conf/opmn.xml` file, as shown:

```
<?xml version = '1.0' encoding = 'UTF-8'?>
  <opmn xmlns="http://www.acme.com/ias-instance">
...
        </ias-component>
```

```
        <ias-component id="OID" status="enabled">
            <process-type id="OID" module-id="OID">
                <environment>
                                            <variable id="ORACLE_SID"
value="value_of_oracle_sid"/>
                                        </environment>
                <stop timeout="1800"/>
                <process-set id="OID" numprocs="1">
                                            <dependencies>
...
</opmn>
```

11. Ensure that the ORACLE_SID environment variable is set to the Oracle Internet Directory replica database.
12. Start the LDAP server and `oidmon` on the replica to be upgraded.
13. Change the password of the replication DN of the upgraded replica by issuing the following command:

    <destination_Infra_OH>/ldap/admin/remtool -presetpwd -v -bind <host>:<port>

14. Start the replication server.
15. Upgrade each of the other master site replicas by performing Steps 2 through 11.
16. Upgrade the database replication table by performing the steps below:
    a. Stop the replication server on all replicas.
    b. Quiesce the replication environment by issuing this command on the MDS replica:

       ***<destination_Infra_OH>*/ldap/admin/remtool -suspendasr**

    c. Connect as `REPADMIN` (the database replication administrator) on the MDS replica and issue the following command:

       execute DBMS_REPCAT.ALTER_MASTER_REPOBJECT (sname=> 'ODS', oname=> 'ASR_CHG_LOG', type=> 'TABLE', ddl_text=> 'alter table ods.asr_chg_log modify target_dn varchar2 (1024)')

    d. Execute the following SQL command repeatedly until the "no rows selected" message appears:

       SELECT * from dba_repcatlog WHERE request = 'ALTER_MASTER_REPOBJECT';

    e. Generate replication support for the ASR_CHG_LOG table by issuing the command:

       execute DBMS_REPCAT.GENERATE_REPLICATION_SUPPORT (sname=> 'ODS', oname=> 'ASR_CHG_LOG', type=> 'TABLE');

    f. Execute the following SQL command repeatedly until the "no rows selected" message appears:

       SELECT * from dba_repcatlog WHERE request = 'ALTER_MASTER_REPOBJECT';

    g. Resume the database replication by issuing the following command:

       ***<destination_Infra_OH>*/ldap/admin/remtool -resumeasr**

    h. Start the replication server on all replicas.

Note: Changes made on the Release 2 (9.0.4) replica may not replicate on the prior version consumer replica. The changes that did not replicate are kept in the Human Intervention Queue for change replication, and will be applied successfully when the consumer replica is upgraded.

Upgrading Oracle Internet Directory on Multiple Replicas Simultaneously

Upgrading multiple replicas simultaneously ensures that the entire network is upgraded without a transient stage. The procedure is simpler than that for upgrading one replica at a time, but involves directory service downtime.

Follow these steps to upgrade multiple replicas simultaneously:

1. Stop the replication server, the LDAP server, and `oidmon` on all replicas in the Directory Replication Group.
2. Stop the database and listener on all replicas in the DRG.
3. Start the Oracle Universal Installer.

   The database and Oracle Internet Directory are upgraded.
4. Start the database and the listener on all replicas.
5. Test the connectivity to other replicas. The Net8 migration assistant might have modified `listener.ora` and `tnsnames.ora`, breaking connectivity. If connectivity is broken, identify the entries that were modified in the files, and restore the entries from the files in `<source_Infra_OH>/network/admin/` to the corresponding files:

   `<destination_Infra_OH>/network/admin/listener.ora`

   `<destination_Infra_OH>/network/admin/sqlnet.ora`

   See Section 3.8.5.3, "Upgrading the tnsnames.ora File" on page 3-60 for instructions and cautions on modifying the `tnsnames.ora` file.
6. Perform the post-upgrade procedures.

   See Also: Section , "Completing the Oracle Internet Directory Upgrade" on page 1-36.
7. Upgrade the database replication table by performing the steps below:
   a. Stop the replication server on all replicas.
   b. Quiesce the replication environment by issuing this command on the MDS replica:

      ```
      <destination_Infra_OH>/ldap/admin/remtool -suspendasr
      ```
   c. Connect as REPADMIN (database replication administrator) on the MDS replica and issue the following command:

      ```
      execute DBMS_REPCAT.ALTER_MASTER_REPOBJECT (sname=> 'ODS',
      oname=> 'ASR_CHG_LOG', type=> 'TABLE', ddl_text=> 'alter
      table ods.asr_chg_log modify target_dn varchar2 (1024)')
      ```
   d. Execute the following SQL command repeatedly until the "no rows selected" message appears:

```
SELECT * from dba_repcatlog WHERE request = 'ALTER_MASTER_
REPOBJECT';
```

e. Generate replication support for the ASR_CHG_LOG table by issuing the command:

```
execute DBMS_REPCAT.GENERATE_REPLICATION_SUPPORT (sname=>
'ODS', oname=> 'ASR_CHG_LOG', type=> 'TABLE');
```

f. Execute the following SQL command repeatedly until the "no rows selected" message appears:

```
SELECT * from dba_repcatlog WHERE request = 'ALTER_MASTER_
REPOBJECT';
```

g. Resume the database replication by issuing the following command:

```
<destination_Infra_OH>/ldap/admin/remtool -resumeasr
```

h. Verify that the replication environment is set up correctly by issuing the following command:

```
<destination_Infra_OH>/ldap/admin/remtool -asrverify [-v
-conn @<repadmin>/<password>@<connect string for the mds
replica>]
```

i. After upgrading the Infrastructure to Oracle Application Server Release 2 (9.0.4), include the ORACLE_SID environment variable in the *<destination_Infra_OH>*/opmn/conf/opmn.xml file, as shown:

```
<?xml version = '1.0' encoding = 'UTF-8'?>
  <opmn xmlns="http://www.acme.com/ias-instance">
...
        </ias-component>
        <ias-component id="OID" status="enabled">
            <process-type id="OID" module-id="OID">
                <environment>
                 <variable id="ORACLE_SID" value="value_of_oracle_sid"/>
                </environment>
                <stop timeout="1800"/>
                <process-set id="OID" numprocs="1">
                 <dependencies>
...
</opmn>
```

j. Change the password of the replication DN by issuing this command on each replica:

```
<destination_Infra_OH>/ldap/admin/remtool -presetpwd -v
-bind <host>:<port>
```

k. Ensure that the ORACLE_SID environment variable is set to the Oracle Internet Directory replica database.

l. Start the replication server, the LDAP server, and oidmon on all the replicas.

Upgrading Oracle Internet Directory v. 9.2.0.x to Release 2 (9.0.4)

Oracle Internet Directory version 9.2.0.x, shipped with the Oracle9i Release 2 database, was a standalone release of Oracle Internet Directory. The Oracle Internet Directory database repository contained only Oracle Internet Directory schema.

The Release 2 (9.0.4) release supports upgrade of a v. 9.2.0.x Oracle Internet Directory deployed with the Oracle 9.2 database repository. Follow the steps below to perform this upgrade.

1. Stop all processes in the Oracle home.
2. Back up the database.
3. If the Oracle Internet Directory database was created with the Oracle9*i* Management and Integration installation type, you must install the Oracle9*i* Database 9.2.0.1.0 Software Only installation type into the same Oracle home, over the database created with the Management and Integration installation type. The Software Only installation type has the options required to use a 9.2 database as a metadata repository.
4. Use the Repository Creation Assistant to convert the 9.2 database to a metadata repository. See Chapter 10, "Installing the OracleAS Metadata Repository in an Existing Database" in the *Oracle Application Server 10g Installation Guide*.

   Note: On the **Register with Oracle Internet Directory** screen of the Repository Creation Assistant, select **Register Later**.

   The metadata repository now has the Release 2 (9.0.4) version of the schema for all OracleAS components except Oracle Internet Directory. The Oracle Internet Directory schema is still at version 9.2.
5. Create the Oracle Internet Directory tablespaces `olts_svrmgstore` and `olts_battrstore` in the 9.2.0.4 Oracle Internet Directory database repository by executing the following SQL statements as `SYS`:

   a. `create tablespace olts_svrmgstore datafile 'svrmg1_oid.dbf' size 1M reuse autoextend on MAXSIZE UNLIMITED EXTENT MANAGEMENT LOCAL;`

   b. `create tablespace olts_battrstore datafile 'battrs1_oid.dbf' size 500K reuse autoextend on EXTENT MANAGEMENT LOCAL AUTOALLOCATE;`
6. Perform a Release 2 (9.0.4) Identity Management-only installation in a separate Oracle home, or on a different computer. (Select Oracle Internet Directory only), specifying the 9.2 database as the metadata repository database.

   See Also: *Oracle Application Server 10g Installation Guide*, Chapter 6, "Installing Oracle Internet Directory Only."

   During the installation, the Oracle Internet Directory Configuration Assistant is invoked. It performs a version check on the Oracle Internet Directory schema; if the version is 9.2.0.x, then it upgrades Oracle Internet Directory to Release 2 (9.0.4). The other configuration tools function as they would when a new installation is performed.

   After the installation, the following conditions are in effect:

   - The Oracle Internet Directory server is running on the non-SSL and SSL ports, as determined by the Release 2 (9.0.4) installation process. The Oracle Internet Directory ports in use are identified in the *<destination_Infra_OH>*`/config/ias.properties`, in the `OIDport` and `OIDsslport` properties.

- The Oracle Internet Directory superuser and Oracle Internet Directory database schema (ODS) password are set to the same value as the `ias_admin` password specified during the Identity Management installation.

7. Set up appropriate access control policies required for the Release 2 (9.0.4) DAS and middle tier installation to operate with the upgraded Oracle Internet Directory by following the steps below:

   a. Create an ldif (`upgrade92.ldif`) file with the entry shown below. Each value of the `orclaci` attribute (shown in bold below) must be a single line, without any line breaks, or an error will occur.

```
#--- BEGIN LDIF file contents---
dn: cn=Attribute Configuration, cn=DAS,cn=Products,cn=OracleContext
changetype: modify
add: orclaci
orclaci: access to entry by group="cn=OracleDASConfiguration,
cn=Groups,cn=OracleContext" (add,delete,browse) by * (noadd,nodelete)
orclaci: access to attr=(*) by group="cn=OracleDASConfiguration, cn=Groups,
cn=OracleContext" (read,write,search,compare) by * (nowrite,nocompare)

dn: cn=Attribute Configuration, cn=DAS,cn=Products,cn=OracleContext,%rlmDN%
changetype: modify
add: orclaci
orclaci: access to entry by group="cn=OracleDASConfiguration,
cn=Groups,cn=OracleContext,%rlmDN%" (add,delete,browse) by *
(noadd,nodelete)
orclaci: access to attr=(*) by group="cn=OracleDASConfiguration, cn=Groups,
cn=OracleContext,%rlmDN%" (read,write,search,compare) by *
(nowrite,nocompare)

#---END LDIF file contents------
```

   b. Replace all occurrences of `%rlmDN%` in the `upgrade92.ldif` with the default realm DN. You can determine the default realm DN with the ldapsearch command shown below:

```
ldapsearch -h <oid host> -p <oid port> -D <OID superuser
DN> -w <OID superuser password> -b
"cn=common,cn=products,cn=oraclecontext" -s base
"objectclass=*" orcldefaultsubscriber
```

   c. Issue the ldapmodify command below:

```
<destination_Infra_OH>/bin/ldapmodify -p <oid port> -h
<oid host> -D <OID superuser name> -w <OID superuser
password> -v -f  upgrade92.ldif
```

8. Perform the tasks in "Completing the Oracle Internet Directory Upgrade" on page 1-36.

Performing Infrastructure Post-Upgrade Tasks

This section details the post-upgrade procedures which will complete the Infrastructure upgrade to Release 2 (9.0.4). It is organized into these sections:

Completing the Oracle Internet Directory Upgrade

To complete the Oracle Internet Directory Upgrade, you should reconfigure all associated OracleAS Portal Release 2 (9.0.4) instances, if applicable, and refresh the Delegated Administration Services (DAS) URL cache. You may also want to execute performance enhancement scripts, and, if applicable, install a new DAS or Directory Integration and Provisioning (DIP) service.

Applying Patches for Portal 9.0.2.2.14 and 9.0.2.3

Some Portal versions require that you apply a patch to the Metadata Repository, as explained below:

- **You are operating Portal version 9.0.2.2.14 (9.0.2 Production in Oracle9iAS 9.0.2.0.1):** You must apply Patch 3238095, which corrects problems with registering users and groups in Oracle9*i*AS Release 2 (9.0.2) Identity Management configuration, and resolves interoperability issues.
- **You are operating Portal 9.0.2.3 (Oracle9iAS 9.0.2.3)**: You must apply Patch 2802414 to resolve interoperability issues.

To apply the patches:

1. Log in to Oracle MetaLink at:

   `http://metalink.oracle.com`

2. Locate the patch specified for the Portal version you are operating.
3. Follow the instructions in the patch Readme file.

Reconfigure the OracleAS Portal Instances for the Oracle Internet Directory Server

If there are any OracleAS Portal Release 2 (9.0.4) instances using the upgraded Oracle Internet Directory server, they should be reconfigured for the Oracle Internet Directory server, as described in Section 4.5.8.2, "Reconfiguring the OracleAS Portal for the Oracle Internet Directory" on page 4-43. This step is required to ensure that the OracleAS Portal entries in Oracle Internet Directory are properly updated, and that t0he correct provisioning events required by Oracle Application Server Release 2 (9.0.4) are sent to the Portal.

Note: This step is required only for the OracleAS Portal Release 2 (9.0.4) instances. If there are multiple instances using the upgraded Oracle Internet Directory server, you must repeat this step for each instance.

Refreshing the Delegated Administration Services (DAS) URL Cache

The URLs for the Delegated Administration Services are different in Oracle9*i*AS Release 2 (9.0.2) Oracle Internet Directory server and the Oracle Application Server Release 2 (9.0.4) Oracle Internet Directory server. When the Oracle Internet Directory server is upgraded, these URLs are updated to the correct values. However, OracleAS Portal maintains a cache of these URLs, which does not get upgraded, and is thus inconsistent with the set of URLs in Release 2 (9.0.4).

The procedure for refreshing the cache is dependent on the version you have. To refresh the cache, follow the steps in one of the sections below.

Refreshing the Cache in Version 9.0.2.6 or Later Follow these steps to refresh the URL cache:

1. Log in to the Portal as a Portal administrator.
2. Click the **Administer** tab.
3. Click the **Global Settings** link in the **Services** portlet.
4. Click the **SSO/OID** tab.
5. Note the values that appear under the section **Cache for OID Parameters**.
6. Click the checkbox next to **Refresh Cache for OID Parameters**.
7. Click **Apply**.
8. Verify that the values displayed under **Cache for OID Parameters** have changed.
9. Click **OK**.

Refreshing the Cache in Versions Prior to 9.0.2.6 Follow these steps to refresh the URL cache:

1. Apply the one-off patch 3225970. This patch is available at:

   `http://metalink.oracle.com`.
2. Clear the Web Cache by performing these steps:
   a. Log in to the Portal as a Portal Administrator.
   b. Click the **Administer** tab.
   c. Click the **Global Settings** link in the **Services** portlet.
   d. Click the **Cache** tab.
   e. Click the checkbox next to **Clear the Entire Web Cache**.
   f. Click **OK**.
3. Clear the middle tier cache by performing these steps:
   a. Navigate to `<destination_MT_OH>/Apache/modplsql/cache`.
   b. Perform a recursive delete of all files under this directory.

Recommended Performance Enhancement Tasks

In Release 2 (9.0.4), Oracle Internet Directory provides some performance enhancements that Oracle Corporation recommends that you implement after upgrading. The implementation involves running two scripts: `oidpu904.sql` and `catalog.sh`, as described below. In the Release 2 (9.0.4) Oracle home:

1. Ensure that the ORACLE_HOME environment variable is set to `<destination_Infra_OH>` and the ORACLE_SID environment variable is set to the infrastructure database SID. If they are not, follow the instructions in "Setting the Environment for Upgrading the Metadata Repository" on page 1-3.
2. Issue this command:

   `sqlplus ods/<ods password>@<net service name for OID database>@<destination_Infra_OH>/ldap/admin/oidpu904.sql`

   for example:

   `sqlplus ods/welcome1@iasdb@<destination_Infra_OH>/ldap/admin/oidpu904.sql`

3. Re-create the index for the `orclnormdn` attribute by executing the `catalog.sh` script, which drops and re-creates the catalog for the `orclnormdn` attribute.

   a. Ensure that the OID server is operating in read-only mode. You can do this with the Oracle Directory Manager.

      See Also: *Oracle Internet Directory Administrator's Guide*, Table C-34, System Operation Attributes (Server Mode field), for instructions on how to make the server operate in read-only mode.

   b. Issue these commands to re-create the index for the `orclnormdn` attribute:

      ```
      <destination_Infra_OH>/ldap/bin/catalog.sh -connect <net service name for OID database> -delete -attr orclnormdn
      ```

      ```
      <destination_Infra_OH>/ldap/bin/catalog.sh -connect <net service name for OID database> -add -attr orclnormdn
      ```

4. Reset the OID server to operate in read-write mode. You can do this with the Oracle Directory Manager.

   See Also: *Oracle Internet Directory Administrator's Guide*, Table C-34, System Operation Attributes (Server Mode field), for instructions on how to make the server operate in read-write mode.

Note: If you had an older version (9.0.2 or 9.2) of DIP operating in a different Oracle home (on a different computer) and using the Oracle Internet Directory you are upgrading now, and you want to continue using the DIP, you must re-register the DIP server. See *Oracle Internet Directory Administrator's Guide* for instructions on registering the DIP server.

Completing the Oracle Application Server Single Sign-On Upgrade

To complete the Oracle Application Server Single Sign-On upgrade, depending on the configuration ugpraded, you may need to perform the tasks below.

Re-configuring the Oracle Application Server Single Sign-On Middle Tier

If the Release 2 (9.0.2) middle tier for the Single Sign-On server had custom configurations (e.g., Oracle HTTP Server configured for SSL, or the Oracle Application Server Single Sign-On server Database Access Descriptor had any custom configuration), then you must re-configure the upgraded Release 2 (9.0.4) middle tier in a like manner.

See Also: *Oracle Application Server Single Sign-On Administrator's Guide*, Chapter 9

Configuring Third-party Authentication

If the Release 2 (9.0.2) middle tier was configured to authenticate with a user certificate or third party authentication mechanism, then you must re-configure the Release 2 (9.0.4) OracleAS Single Sign-On server in a like manner.

See Also: *Oracle Application Server Single Sign-On Administrator's Guide*, Chapter 13

Installing Customized Pages in the Upgraded Server

If you have customized the login, password and the sign-off pages in the Release 2 (9.0.2) Single Sign-On server, then you must update those pages with Release 2 (9.0.4) specifications.

> **See Also:** *Oracle Application Server Single Sign-On Administrator's Guide*, Chapter 12

Converting External Application IDs

> **Note:** You do not need to perform this task if you upgraded from an OracleAS Single Sign-On version of 9.0.2.5 or later.

To avoid ID conflicts while exporting and importing external application data among multiple OracleAS Single Sign-On server instances, external application IDs must be unique. In the Release 2 (9.0.2) release, external application IDs were sequential, and not unique across instances. If you are upgrading from Release 2 (9.0.2) directly to Release 2 (9.0.4), then you must convert existing short external application IDs to the longer format in the OracleAS Single Sign-On schema. Follow the steps below to convert the IDs:

1. Execute the `orasso` script from the OracleAS Single Sign-On schema directory using these commands:

   ```
   sqlplus orasso/<password>

   spool extappid.log

   @?/sso/admin/plsql/sso/ssoupeid.sql

   spool off
   ```

   If you have OracleAS Portal versions that are lower than 9.0.2.6 and that use the upgraded OracleAS Single Sign-On server, then you must apply patches to each instance according to the table below. Patches are available at:

   http://metalink.oracle.com

   > **Note:** You might need the `SSO_IDENTIFIER` value to apply the patches, if the value cannot be generated in the OracleAS Portal schema automatically, or if the OracleAS Single Sign-On server used a randomly selected value for the SSO_IDENTIFIER.

Table 1–1 OracleAS Portal Patches for Converting to Long Format Application IDs

OracleAS Portal Version	Patch Number
3.0.9.8.4	2769007
3.0.9.8.5	2665597
9.0.2, 9.0.2.3	2665607

Setting Up OracleAS Single Sign-On Replication

If you are using Oracle Internet Directory replication and want to also use OracleAS Single Sign-On replication, add the upgraded Release 2 (9.0.4) tables in the replication

group along with 9.0.4 OID. Follow the steps below to add OracleAS Single Sign-On tables for replication:

1. Stop the Oracle Internet Directory replication server on all replicas of the Directory Replication Group.
2. On the Master Directory replica, in *$ORACLE_HOME*/ldap/admin, issue the following command:

   sqlplus repadmin/<*password*>@<*mds connect id*> @oidrssou.sql

3. Start the Oracle Internet Directory replication server on all replicas of the Directory Replication Group.

   See Also: *Oracle Internet Directory Administrator's Guide*, Chapter 25, Managing Directory Replication

Upgrading the OracleAS Single Sign-On Server with a Customized Middle Tier

If the Release 2 (9.0.2) OracleAS Single Sign-On server was using a middle tier other than the default mid-tier installation along with the OracleAS Single Sign-On server, then you must configure that middle tier to point to the upgraded OracleAS Single Sign-On server. For example, if there was a reverse proxy configured in the Release 2 (9.0.2) OracleAS Single Sign-On server middle tier, then you must configure it on the Release 2 (9.0.4) OracleAS Single Sign-On server middle tier.

Troubleshooting Wireless Voice Authentication

If you want to use wireless voice authentication with the Release 2 (9.0.4) OracleAS Single Sign-On server, and it doesn't work, verify that the OracleAS Single Sign-On server entry is a member of the Verifier Services Group in Oracle Internet Directory (`cn=verifierServices,cn=Groups,cn=OracleContext`). This is a requirement for the wireless voice authentication feature. Follow the steps below to verify membership:

1. Issue the following command:

   ldapsearch -h <*host*> -p <*port*> -D cn=orcladmin -w <*password*> -b "cn=verifierServices,cn=Groups,cn=OracleContext" "objectclass=*"

   The OracleAS Single Sign-On server is a member of the Verifier Services Group if it is listed as a `uniquemember` in the entry, as shown in Example 1–1.

Example 1–1 OracleAS Single Sign-On Server uniquemember Listing

```
cn=verifierServices, cn=Groups,cn=OracleContext
.
.
.
uniquemember=orclApplication
CommonName=ORASSO_SSOSERVER,cn=SSO,cn=Products,cn=OracleContext
.
.
.
```

Installing Languages in the OracleAS Single Sign-On Server

If you did not select any languages during the OracleAS Single Sign-On upgrade, or you want to install additional languages after the upgrade, you can install the necessary languages by following the steps below.

1. Copy the necessary language files from the Repository Creation Assistant CD-ROM Oracle home to the OracleAS Single Sign-On server Oracle home:

   cp <repCA_CD>/portal/admin/plsql/nlsres/ctl/<lang>/*.* <destination_Infra_OH>/sso/nlsres/ctl/<lang>/

   where *<lang>* is the language code. For example, the language code for Japanese is `ja`.

2. Load the languages into the server.

> **See Also:** *Oracle Application Server Single Sign-On Administrator's Guide*, Chapter 2, "Configuring Globalization Support" section.

Re-Registering OracleAS Portal with the Upgraded OracleAS Single Sign-On Server

After performing a distributed Identity Management upgrade (depicted in Figure 1–2 and Figure 1–3) from Oracle9*i*AS Release 2 (9.0.2) to Oracle Application Server Release 2 (9.0.4), the OracleAS Single Sign-On schemas are relocated in the Oracle Internet Directory database. OracleAS Portal keeps a database link reference to the OracleAS Single Sign-On server password store schema `ORASSO_PS`. This link reference must be updated. To do this, re-register the corresponding OracleAS Portal with the upgraded OracleAS Single Sign-On server.

> **See Also:** *Oracle Application Server Portal Configuration Guide*, Appendix B.

Re-Registering mod_osso with the Upgraded OracleAS Single Sign-On Server

After performing a distributed Identity Management upgrade (depicted in Figure 1–2 and Figure 1–3) from Oracle9*i*AS Release 2 (9.0.2) to Oracle Application Server Release 2 (9.0.4), you may need to re-register `mod_osso` in order for an Oracle9*i*AS Release 2 (9.0.2) middle tier to operate with the upgraded OracleAS Single Sign-On server. You will need to do this if the Oracle HTTP Server host and port information for mod_osso was changed. Before re-registering `mod_osso`, you must first set the value of the `ColocatedDBCommonName` attribute in the *<source_MT_OH>*`/config/ias.properties` file to the global database name of the new OracleAS Single Sign-On server database shared with Oracle Internet Directory (for example, `iasdb.host.mydomain`).

Using an Upgraded Identity Management Configuration with Oracle9*i*AS Discoverer Release 2 (9.0.2)

If you upgraded an Identity Management configuration that was in use by Oracle9*i*AS Discoverer Release 2 (9.0.2), and you want to continue operating Oracle9*i*AS Discoverer Release 2 (9.0.2) with the upgraded Identity Management, then you must change the value of the `ColocatedDBCommonName` attribute in the *<source_MT_OH>*`/config/ias.properties` file. The value must be changed to the global database name of the database used by the upgraded Oracle Internet Directory (e.g., *`iasdb.oid_host_name.domain`*).

Completing the Oracle Application Server Wireless Upgrade

This section describes the tasks you must perform in order to complete the Oracle Application Server Wireless upgrade.

Upgrading Wireless User Accounts in Oracle Internet Directory

In Oracle Application Server Wireless Release 2 (9.0.2), user account numbers and PINs for wireless voice authentication were stored in the Wireless repository.

In Oracle Application Server Wireless Release 2 (9.0.4), new attributes are added in the object definition of the `orcluserV2` object class of Oracle Internet Directory to store the account number and PIN. As part of the Oracle Application Server Wireless upgrade from Release 2 (9.0.2) to Release 2 (9.0.4), user account numbers and PINs must be transferred from the Wireless repository to Oracle Internet Directory.

This upgrade step can be performed only after the Oracle Application Server Infrastructure and all middle tiers are upgraded to Release 2 (9.0.4). If they are not performed, the Oracle Application Server Wireless server will continue to authenticate voice devices locally (without Oracle Application Server Single Sign-On).

To upgrade the account numbers and PINs:

1. Issue the command:

   <destination_MT_OH>*/wireless/bin/migrate902VoiceAttrsToOID.sh *<destination_MT_OH>* *<ldapmodify location>* *<userdn>* *<password>* *<ldif file location>* *<log file>

   where:

   - *<ldapmodify location>* is the location of the `ldapmodify` utility (usually *<destination_MT_OH>*`/bin`)
   - *<user dn>* is the DN of the Oracle Internet Directory administrator user
   - *<password>* is the password of the Oracle Internet Directory administrator user
   - *<ldif file location>* is the absolute path to the ldif (Lightweight Directory Interchange Format) file. This file contains user account numbers and PINs and is uploaded to Oracle Internet Directory by the `ldapmodify` utility. This temporary file may be removed after the user upgrade procedure has been completed successfully.
   - *<log file>* is the absolute path to the log file

Example:

```
migrate902VoiceAttrsToOID.sh /private/ias904/
/private/ias904/bin/ldapmodify cn=orcladmin welcome1
/private/ias904/users.ldif /private/ias904/users.log
```

Adding Unique Constraint on the orclWirelessAccountNumber Attribute in Oracle Internet Directory

In Release 2 (9.0.4), Oracle Internet Directory does not automatically set unique constraints on any user attributes. Wireless voice authentication will not function properly unless a unique constraint is set on the `orclWirelessAccountNumber` attribute of the `orclUserV2` object class.

Set the unique constraint by performing the steps below after the middle tier and infrastructure upgrades are complete.

1. Execute *<destination_MT_OH>*`/wireless/bin/addAccountNumberUniqueConstraint.sh`. The script takes one argument, the full path to the Oracle home. For example:

   `addAccountNumberUniqueConstraint.sh` *<destination_MT_OH>*

2. Restart the Oracle Internet Directory server.

Disabling Oracle Application Server Wireless Upgrade Triggers in the Infrastructure Repository

When Oracle Application Server Wireless Release 2 (9.0.4) is installed against an Oracle9iAS Release 2 (9.0.2) infrastructure, a number of triggers are automatically installed, that ensure that both Oracle9iAS Wireless Release 2 (9.0.2) and Oracle Application Server Wireless Release 2 (9.0.4) middle tiers can function correctly. Once all Oracle9iAS Wireless Release 2 (9.0.2) middle tiers and the infrastructure tier have been upgraded to Oracle Application Server Wireless Release 2 (9.0.4), you must execute the following script to disable any upgrade-related triggers.

```
disable902-904_trg.sh
```

This script is located in the <*destination_MT_OH*>/wireless/bin directory. You must set the ORACLE_HOME environment variable before you execute the script.

Activating All Oracle Application Server Wireless Release 2 (9.0.4) Features

When Oracle Application Server Wireless Release 2 (9.0.4) is installed against an Oracle9iAS Release 2 (9.0.2) Infrastructure, a number of features are disabled by default, as they are not compatible with existing Oracle9iAS Wireless Release 2 (9.0.2) middle tiers that are installed against the same Infrastructure. After all Oracle9iAS Wireless Release 2 (9.0.2) middle tiers have been upgraded to Oracle Application Server Wireless 10*g* (9.0.4), you can manually enable these features. Once you have enabled these features, the Oracle9iAS Wireless Release 2 (9.0.2) middle tiers will no longer function correctly.

Enable the Oracle Application Server Wireless Release 2 (9.0.4) features by executing the following script from any of the Oracle Application Server Wireless Release 2 (9.0.4) middle tiers, using the command below. This script is in the <*destination_MT_OH*>/wireless/bin directory.

upload.sh ../repository/xml/activate-9040.xml -l <*wireless user name*>/<*password*>

where:

- <*wireless user name*> is the name of the Oracle Application Server Wireless user
- <*password*> is the password of the Oracle Internet Administrator

For example:

```
upload.sh  ../repository/xml/activate-9040.xml -l
orcladmin/welcome1
```

Assigning Change Password Privilege to OracleAS Wireless

In Oracle Application Server Release 2 (9.0.4), by default, the OracleAS Wireless application entity does not have the privileges to change the user password. Consequently, upon installation, users cannot change the password to the OracleAS Wireless server. However, you can enable functionality to change passwords by assigning the `UserSecurityAdmins` privilege to the OracleAS Wireless application entity.

To do this, execute the script <*destination_MT_OH*>wireless/bin/assignUserSecurityAdminsPrivilege.sh

The syntax is:

```
assignUserSecurityAdminsPrivilege.sh <oid super user dn> <user
password>
```

where:

- *<oid super user dn>* is the Distinguished Name of the Oracle Internet Directory super user. This user should have privileges to grant UserSecurityAdmins privileges to application entities.
- *<user password>* is the password of the Oracle Internet Directory super user.

For example:

```
assignUserSecurityAdminsPrivilege.sh cn=orcladmin welcome1
```

Specifying URL Query Parameters for Wireless Services That Use the HTTP Adapter

When you use the HTTP adapter to build Wireless services, one of the service parameters that you must specify is the URL to a back-end application. In some cases, you may send some query parameters to the back-end application. There are two ways to do this from OracleAS Wireless, shown in Example 1–2 and Example 1–3. In Example 1–2, the parameter name is `fn` and the value is `Joe`.

Example 1–2 URL Using a Query Parameter

```
http://localhost:7777/myapp/home.jsp?fn=Joe
```

The query parameter is sent only in the request for the first page of that service. If there is a link from the first page to some other pages, then the parameter is not added to the request for those pages.

Example 1–3 URL Using an Extra Service Parameter

```
http://localhost:7777/myapp/home.jsp
```

Instead of modifying the URL, you add an extra service parameter with name `fn` and value `Joe`. The the parameter is sent to all pages, not just the first one. The parameter is also sent with all HTTP redirect requests. However, this method also sends extra URL parameters to the OracleAS Single Sign-On server, which causes the server to return an error.

The error occurs when the back-end application is protected by mod_osso. In that case, the request to that application is intercepted and redirected to the Oracle SSO server for user authentication. The OracleAS Single Sign-On server has restrictive rules concerning query parameters that can be sent to it. Consequently, for back-end applications protected by mod_osso, you must change the Wireless service and add the query parameter to the URL as shown in Example 1–2.

Decommissioning the Release 2 (9.0.2) Oracle Home

After you complete the Identity Management upgrade, you will probably want to consider relocating the database files to a location outside of the source Oracle home. Even after the Identify Managment upgrade is complete, the database files still remain in the source Oracle home. If you decide to deinstall the source Oracle home, these database files will still remain there unless you take steps to relocate them. It is a good idea to relocate the files as a safeguard against inadvertently deleting them (for example, by deleting the entire source Oracle home directory tree). In addition, there

may be performance benefits to moving the database files outside of the source Oracle home.

After the database files have been relocated and the software in the source Oracle home has been deinstalled, then you may safely delete the entire source Oracle home directory tree.

This procedure is intended to be performed by a database administrator, and is described in greater detail in the *Oracle9i Database Administrator's Guide*.

Deinstalling Oracle9*i*AS Release 2 (9.0.2) and Deleting the Source Oracle Home

If you have relocated the Release 2 (9.0.2) files, you may wish to delete the old Oracle home. To do this, deinstall the Release 2 (9.0.2) infrastructure instance in the source Oracle home using the same version of Oracle Universal Installer that was used to install it, or a later version, and then delete all files from `<source_Infra_OH>`.

Deinstalling an Oracle9*i*AS Release 2 (9.0.2) or (9.0.3) instance when there is also an OracleAS Release 2 (9.0.4) instance on the computer requires a patch. Before you deinstall such an instance, be aware of the issues associated with this deinstallation that may apply to your configuration.

> **See Also:** *Oracle Application Server 10g Installation Guide* for information on deinstalling a Release 2 (9.0.2) or (9.0.3) instance when a 10*g* (9.0.4) instance exists on the same computer.

Relocating Data, Control, and Log Files

Follow these steps to relocate data, control, and log files.

1. Create a directory for the relocated files in a location that is separate from the source Infrastructure Oracle home.
2. Copy all data files to the directory created in Step 1.

   > **See Also:** *Oracle9i Database Administrator's Guide*, section titled "Renaming and Relocating Datafiles"

3. Copy all log files to the directory created in Step 1.

   > **See Also:** *Oracle9i Database Administrator's Guide*, section titled "Renaming and Relocating Datafiles"

4. Relocate all control files to the directory created in Step 1.

   > **See Also:** *Oracle9i Database Administrator's Guide*, section titled "Creating Additional Copies, Renaming, and Relocating Control Files"

Validating the Identity Management Upgrade

This section describes the steps you must perform after the Identity Management Upgrade to ensure that the upgrade was successful.

Executing the utlrp.sql Utility

You must run the `utlrp.sql` utility as a post-installation step. This PL/SQL procedure recompiles all PL/SQL packages that may have been invalidated during the upgrade to Release 2 (9.0.4). To run this utility, do the following:

1. Ensure that the upgraded Metadata Repository database is running.
2. Ensure that the ORACLE_HOME environment variable is set to <*Infra_OH*> and the ORACLE_SID environment variable is set to the Infrastructure database SID. If they are not, follow the instructions in "Setting the Environment for Upgrading the Metadata Repository" on page 1-3.
3. Connect to the database in the destination Infrastructure Oracle home as SYS as SYSDBA in single user mode.
4. Issue the following command at the SQL*Plus prompt:

```
@?/rdbms/admin/utlrp.sql
```

Checking for Invalid Database Objects

Follow these steps to ensure that none of the database objects that are required by Oracle Application Server are invalid:

1. Connect to the database in the destination Infrastructure Oracle home as SYSDBA.
2. Issue the following command:

```
SELECT owner, object_type, object_name
 FROM all_objects
 WHERE status='INVALID';
```

The query should not return any database objects that have an Oracle Application Server component schema (such as PORTAL, WIRELESS, etc.) in the 'owner' column.

Testing Oracle Application Server Single Sign-On Connectivity

After the Identity Management upgrade is complete, log in to Oracle Application Server Single Sign-On as user ORCLADMIN. A successful login indicates that Oracle Application Server Single Sign-On and Oracle Internet Directory are functioning after the Identity Management upgrade.

1. In a browser, access the Oracle Enterprise Manager in the destination Infrastructure Oracle home by entering its URL. Ensure that you provide the correct host name and port number. For example:

   `http://infrahost.mycompany.com:1812`

   The Oracle Enterprise Manager page displays, withthe Oracle Application Server Release 2 (9.0.4) Identity Management instance in the **Standalone Instances** section.
2. Click the link for the Identity Management instance.

   The **System Components** page appears.
3. Verify that the status of the Oracle HTTP Server, Oracle Internet Directory, and Oracle Application Server Single Sign-On components is **Up**.
4. In the browser, access the ORASSO page by entering its URL. Ensure that you enter the correct host name and port number for the upgraded Oracle HTTP Server. For example:

```
http://infrahost.mycompany.com:7777/pls/orasso/ORASSO.home
```

The ORASSO page appears.

5. Click the **Login** link (in the upper right corner of the page).

   A page appears with **User Name** and **Password** fields.

6. Enter ORCLADMIN in the User Name field, and the password you have selected for ORCLADMIN in the Password field.

7. Click **Login**.

   The Oracle Application Server Single Sign-On Server **Administration** page appears, thus validating the basic operation of the upgraded Identity Management components (Oracle Application Server Single Sign-On and Oracle Internet Directory).

2

Integration with the Microsoft Windows Environment

Oracle provides centralized security administration for all Oracle components by tightly integrating them with Oracle Identity Management. Similarly, Microsoft provides centralized security administration in Windows 2000 and Microsoft Windows NT by tightly integrating all Microsoft applications with Microsoft Active Directory.

This chapter, written for environments with both Oracle and Microsoft technology stacks, explains how Oracle Identity Management can integrate with Microsoft Windows environments. It contains these topics:

> **See Also:** "Oracle Internet Directory Frequently Asked Questions" on the Oracle Technology Network at
>
> `http://otn.oracle.com`

Overview of Integration with the Microsoft Windows Environments

This section discusses the various aspects of the Windows integration environment as well as the Oracle components and tools involved. It contains these topics:

Components for Integrating with the Microsoft Windows Environment

Table 2–1 describes each Oracle component used in integrating Oracle Internet Directory with Microsoft Active Directory.

Table 2–1 Components for Integrating with Microsoft Active Directory

Component	Description
Oracle Internet Directory	The repository in which Oracle components and third-party applications store and access user identities and credentials. It uses the Oracle directory server to authenticate users against the stored credentials. When credentials are stored in a third-party directory and not in Oracle Internet Directory, users can still be authenticated. In this case, Oracle Internet Directory uses an external authentication plug-in that goes to the third-party directory server for authentication.
Oracle Directory Integration and Provisioning Platform	This platform enables: ■ Synchronization between Oracle Internet Directory and other directories and user repositories ■ Automatic provisioning services for Oracle components It is installed as part of the Oracle Application Server infrastructure, but you can install it separately. This platform includes connectors for synchronizing between Oracle Internet Directory and other LDAP directories. One of its connectors, the Active Directory connector, is designed for two-way synchronization between Oracle Internet Directory and Microsoft Active Directory. The Active Directory connector enables you to: ■ Configure either one-way or two-way synchronization. ■ Designate a specific subset of attributes for synchronization. You do this by configuring the appropriate mapping rules, which you can then change at runtime. ■ Synchronize against multiple Microsoft Active Directory servers. You can synchronize changes both directly against an individual server and from an entire Microsoft Active Directory environment by using the Microsoft Global Catalog. You cannot synchronize user data between Oracle Internet Directory and Microsoft Windows NT by using the Oracle Directory Integration and Provisioning platform. You can, however, achieve this synchronization indirectly by synchronizing first between Oracle Internet Directory and Microsoft Active Directory, and then between Microsoft Active Directory and Microsoft Windows NT.

Table 2–1 (Cont.) Components for Integrating with Microsoft Active Directory

Component	Description
Directory Integration and Provisioning Assistant	This tool enables you to migrate data between Oracle Internet Directory and a third-party directory. More specifically, it enables you to: ■ Migrate data in either direction ■ Migrate a large set of data by using an LDIF file, or a smaller set of data by using straight LDAP ■ Migrate all or a subset of attributes within each entry. This tool uses the same set of mapping rules as the Oracle directory integration and provisioning server. You cannot directly load user data from Oracle Internet Directory into Microsoft Windows NT by using the Directory Integration and Provisioning Assistant. You can, however, achieve this indirectly by first loading the data into Microsoft Active Directory, and then using Microsoft tools to load the data from Microsoft Active Directory into Microsoft Windows NT.
Oracle Application Server Single Sign-On	Oracle Application Server Single Sign-On enables users to access Oracle Web-based components by logging in only once. Oracle components delegate the login function to the OracleAS Single Sign-On server. When a user first logs into an Oracle component, the component redirects the login to the OracleAS Single Sign-On server. The OracleAS Single Sign-On server authenticates the user by verifying the credentials entered by the user against those stored in Oracle Internet Directory. After it has authenticated the user, and throughout the rest of the session, the OracleAS Single Sign-On server grants the user access to all the components the user seeks and is authorized to use. Oracle Application Server Single Sign-On enables native authentication, also called autologin, in a Microsoft Windows environment. Once logged into the Windows desktop, the user automatically has access to Oracle components. OracleAS Single Sign-On automatically logs the user into the Oracle environment using user's Kerberos credentials.
Active Directory External Authentication Plug-in	This plug-in, which is part of the Oracle directory server, enables Microsoft Windows users to log into the Oracle environment by using their Microsoft Windows credentials. When such a user tries to log in, the OracleAS Single Sign-On server tries to verify the credentials the user enters against those stored in Oracle Internet Directory. If the user credentials are not there, then the Oracle directory server invokes the Active Directory external authentication plug-in. This plug-in verifies the user credentials in Microsoft Windows. If the verification is successful, then the Oracle directory server notifies the OracleAS Single Sign-On accordingly. In addition to enabling external authentication against Microsoft Windows, this plug-in also automatically provisions Microsoft Windows users into the Oracle Identity Management system.
Oracle Internet Directory Self-Service Console	Oracle Internet Directory Self-Service Console is a Web-based tool for managing users, groups, and their credentials in Oracle Internet Directory. Built from service units of Oracle Delegated Administration Services, this tool enables users to manage user passwords and password policies. **See Also:** *Oracle Internet Directory Administrator's Guide*, Chapter 31, "Oracle Internet Directory Self-Service Console" for details on how to use this tool to manage realms and user and group search bases

Table 2–1 (Cont.) Components for Integrating with Microsoft Active Directory

Component	Description
Oracle Directory Manager	Oracle Directory Manager is a Java-based tool for administering Oracle Internet Directory. It enables directory administrators to manage all directory data including user information and configuration information used by the Oracle directory integration and provisioning server.

Methods for Tracking Changes in Microsoft Active Directory

Microsoft Active Directory provides various ways of tracking changes to its directory contents. Two of these approaches are:

- The DirSync control-based approach
- The USNChanged-based approach

In each approach, the directory from which changes are derived is polled at scheduled intervals by the Active Directory connector.

Each approach has advantages and disadvantages. Table 2–2 compares and contrasts the two approaches.

Table 2–2 Comparing and Contrasting the DirSync Approach with the USNChanged Approach

Consideration	DirSync Approach	USNChanged Approach
Change key	Presents changes to the `ObjectGUID`-the unique identifier of the entry	Presents changes to the distinguished name. The `ObjectGUID` is used to keep track of modifications of the RDN.
Changes to multivalued attributes	Reflects incremental changes made to multivalued attributes as a complete replacement of the attribute value. This might cause unnecessary traffic on the network.	Reflects incremental changes made to multivalued attributes as a complete replacement of the attribute value. This might cause a lot of unnecessary traffic on the network.
Error handling	If synchronization aborts, starts the next cycle from the current place. This requires keeping count of the number of changes applied during any synchronization operation. Otherwise, some changes are applied again.	Does not require synchronization to be atomic. If synchronization of a particular entry fails, then the next synchronization cycle can start from the current or next entry.
Information in the search results	Provides search results consisting of only the changed attributes and the new values. Application of these changes to Oracle Internet Directory is very easy.	Provides search results consisting of the complete changed entry. All the attribute values are compared to the old values stored in Oracle Internet Directory and applied, only if it has changed. This can be time consuming.
Information in the search results	Provides search results consisting of only the changed attributes and the new values. Application of these changes to Oracle Internet Directory is very easy.	Provides search results consisting of the complete changed entry. All the attribute values are compared to the old values stored in Oracle Internet Directory and applied, only if it has changed. This can be time consuming.
Monitoring of applied changes	When queried for changes in the directory, presents incremental changes based on a cookie value that identifies the state of the directory. Because the cookie is a binary value, changes over a period of time cannot be selectively ignored.	The changes are queried in the directory based on the USNChanged attribute, which is an Integer. It is very easy to modify the value if required.

Table 2–2 (Cont.) Comparing and Contrasting the DirSync Approach with the USNChanged Approach

Consideration	DirSync Approach	USNChanged Approach
Privileges required for the synchronizing user	Requires the user to have the `SE_SYNC_AGENT_NAME` privilege, which enables reading all objects and attributes in Microsoft Active Directory regardless of the access protections on the objects and attributes.	No special privileges required. The user must have privileges to read and write in the specific container.
Support of multiple domains	Requires separately connecting to the different domain controllers to read changes made to the entries in different domains.	Enables the user to read changes made to the multiple domains by connecting to the Global Catalog Server.
Synchronization from a replicated directory in case of failover	Can be continued as it is. The synchronization key is the same when connecting to a replicated environment.	Requires the change number to be updated before starting synchronization with the failover directory.
Synchronization scope	Reads all the changes made in the directory, filters out the changes made to the required entries, and propagates to Oracle Internet Directory.	Makes it possible to look for changes in any specific subtree.
Two-way Synchronization	For two-way synchronization, requires configuring an import profile and an export profile for each of the domain controllers.	For two way synchronization, requires one profile for importing changes from all the domain controllers, and individual profiles to export changes to each of the domain controllers.
Usability in an environment with multiple Microsoft Active Directory servers behind a load balancer	Connect to a specific Microsoft Active Directory node, preferably a Global Catalog Server.	Connect to a specific Microsoft Active Directory node.

Configuration Information Set During Installation of the Active Directory Connector

During installation, default synchronization profiles, mapping rules, and access controls are preconfigured. You can customize them to meet the needs of your deployment.

Synchronization Profiles

Most of the information for enabling synchronization is preconfigured in Oracle Internet Directory during installation and stored in a directory entry called `Synchronization Profile`. This information is used by the Oracle directory integration and provisioning server during synchronization and by the Directory Integration and Provisioning Assistant during bootstrapping.

You can change this information at runtime to meet your requirements. The next time the directory integration and provisioning server uses the profile for synchronization, it automatically refreshes its cache with the changed information. This saves you from restarting this server every time you change configuration information.

During installation, three default Active Directory synchronization profiles are created in Oracle Internet Directory. You can use them for running the Active Directory connector if they are adequate for your needs. Otherwise, use them as templates, customizing them to meet the needs of your deployment. They are:

- `ActiveImport`-The profile for importing changes from Microsoft Active Directory to Oracle Internet Directory by using the DirSync approach

- `ActiveChgImp`-The profile for importing changes from Microsoft Active Directory to Oracle Internet Directory by using the USNChanged approach
- `ActiveExport`-The profile for exporting changes from Oracle Internet Directory to Microsoft Active Directory.

Mapping Rules

Mapping rules, an important part of the synchronization profile, determine what directory information is to be synchronized from one directory to another and how it is to be synchronized. You can change mapping rules at runtime to meet your requirements.

Default Mapping Rules with Default User and Group Attributes Each default Active Directory synchronization profile includes default mapping rules. These rules contain a minimal set of default user and group attributes configured for synchronization out of the box. These default attributes are described in Table 2–3, which lists them using their respective names in Microsoft Active Directory and Oracle Internet Directory.

Table 2–3 Default User and Group Attributes

Name in Microsoft Active Directory	Name in Oracle Internet Directory	Description
Default User Attributes		
`cn`	`cn`	User name
`SAMAccountName`	`user:orclADSAMAccountName`	Contains Microsoft Active Directory login ID. Used by Oracle Application Server Single Sign-On Service for Windows native Authentication.
`UserprinicipalName`	`uid`	Used by Oracle Application Server Single Sign-On Service for single sign-on
`UserprinicipalName`	`orclADUserprinicipalName`	Used by Oracle Application Server Single Sign-On Service for single sign-on in case `uid` can not be used
`ObjectGUID`	`orclADObjectGUID`	Used by Active Directory Connector as Synchronization key
`ObjectSID`	`orclsADObjectSID`	Not used currently
Default Group Attributes		
`cn`	`cn`	User name
`SAMAccountName`	`user:orclADSAMAccountName`	Contains Microsoft Active Directory login ID
`Managedby`	`Owner`	Represents who owns the group entry
`Member`	`uniquememeber`	Represents DNs of member users in the groups

In addition to the default attributes in Table 2–3, the `ou` (organizational unit) attribute is also preconfigured for synchronization. It is represented by ou both in Microsoft Active Directory and Oracle Internet Directory.

Access Controls

To enable users to access only data they are authorized to use, proper access controls are required in Oracle Internet Directory. More specifically, access controls are required to:

- Enable only the authorized accounts to create data in Oracle Internet Directory when synchronizing it from Microsoft Active Directory
- Allow only the user and group objects to be created in the proper containers

Two default access control policies are preconfigured during installation. They ensure that only authorized users can create entries in Oracle Internet Directory. The first policy disallows creation of any objects except users under the users subtree, which is the default container for all users to be synchronized. The second policy disallows creation of any objects except groups under the groups subtree, which is the default container for all groups to be synchronized.

> **See Also:** "Directory Information Tree Setup for Integration with Microsoft Active Directory" on page 2-8 for more details on the user and group subtrees

Information Required During Setup

After installation of Oracle Internet Directory, you need to configure only minimal additional information in the synchronization profile to enable synchronization between the two directories. In a simple deployment, you can easily configure this information by using the script `adprofilecfg.sh`. Other tools for configuring the information are:

- Oracle Internet Directory Self-Service Console, described in Chapter 31, "Oracle Internet Directory Self-Service Console" of the *Oracle Internet Directory Administrator's Guide*
- Directory Integration and Provisioning Assistant, described in "Directory Integration and Provisioning Assistant" on page 2-3
- Oracle Directory Manager, described in Chapter 4, "Directory Administration Tools" of the *Oracle Internet Directory Administrator's Guide*

> **See Also:** "Configuring the Active Directory Connector" on page 2-15 for a detailed description of the information you need to configure to enable the synchronization

Information Required in a Multiple-Domain Microsoft Active Directory Environment

Information Required for Synchronizing from Microsoft Active Directory to Oracle Internet Directory

Configuration information required in multiple-domain Microsoft Active Directory environments for synchronizing Microsoft Directory to Oracle Internet Directory depends on whether the Global Catalog is configured. If it is available, then the Active Directory connector can synchronize from the Global Catalog. In this case, you must configure only one synchronization profile. If the Global Catalog is not available, then the Active Directory connector must go to each Microsoft Active Directory server to synchronize from Microsoft Active Directory. In this case, you must configure as many export profiles as there are number of Microsoft Active Directory domains.

Information Required for Synchronizing from Oracle Internet Directory to Microsoft Active Directory

Configuration information required in multiple-domain Microsoft Active Directory environments for synchronizing from Oracle Internet Directory to Microsoft Active Directory does not depend on the Global Catalog. The Active Directory connector always goes to each Active Directory to synchronize from Oracle Internet Directory to Microsoft Active Directory. You must configure as many export profiles as there are Microsoft Active Directory domains.

> **See Also:** "Configuring the Active Directory Connector" on page 2-15 and "Configuring the Active Directory Connector" on page 2-15 for instructions on configuring synchronization in environments with multiple Microsoft Active Directory domains

Directory Information Tree Setup for Integration with Microsoft Active Directory

Information in an LDAP directory is organized in a Directory Information Tree (DIT). In this tree, each node is called a directory entry that is identified by a unique value, called a distinguished name (DN).

A part of a tree that serves as a container for other entries is called a subtree. A node of a tree that contains no other entries is called a leaf.

Users and groups are represented as entries and can be either leaf or non-leaf nodes.

To facilitate proper organization of information and to enforce proper access controls in the directory, a top-level DIT structure is configured in the directory during installation. For example, the domain of Oracle Internet Directory is `us.MyCompany.com`, and a pre-configured default realm value is chosen during installation, then, after installation, the Oracle Internet Directory Configuration Assistant configures a default DIT. This default DIT, shown in Figure 2–1, contains two special entries: `users` and `groups`. These two entries are the roots of the two subtrees containing users and groups.

Planning the Directory Information Tree

The most important decisions to be made before synchronization are:

- What information to synchronize

  You can synchronize either the entire DIT or part of it.

- Where to synchronize

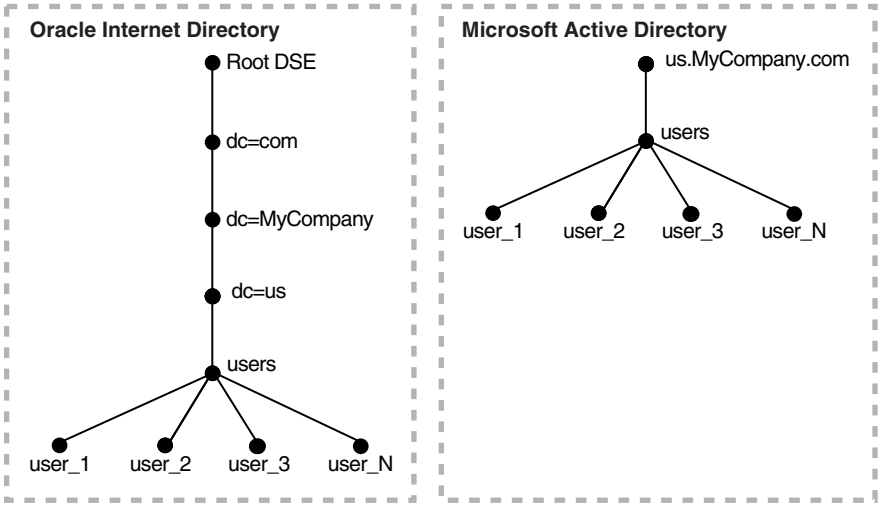
  The Active Directory connector enables you to choose from two possible configurations:

  – Synchronizing so that the relative position of each entry in the DIT is the same in both the source and destination directories. This configuration, called one-to-one domain mapping, is the most commonly used configuration. It is also the recommended configuration.

  – Synchronizing so that the relative position of each entry in the DIT is different in the destination directory from that in the source directory. In this configuration, whenever information is synchronized, you must change the DN values of all entries being mapped, including their references in group entries. Doing this can be very expensive.

Figure 2–1 shows an example of one-to-one mapping between the DITs in two directories.

Figure 2–1 Default DIT Structures in Oracle Internet Directory and Microsoft Active Directory when Both Directory Hosts are Under the Domain us.MyCompany.com



In the deployment illustrated in Figure 2–1:

- Both Microsoft Active Directory and Oracle Internet Directory hosts are in the same domain, namely, `us.MyCompany.com`.
- Users are synchronized only from Microsoft Active Directory to Oracle Internet Directory. All users to be synchronized are stored in one container in Microsoft Active Directory, namely, `users.us.MyCompany.com`.
- The same DIT structure is maintained in both Microsoft Active Directory and Oracle Internet Directory. All the users appear in the same users subtree identified by the value `users.us.MyCompany.com`.

In such a deployment, only the users subtree must be synchronized from Microsoft Active Directory to Oracle Internet Directory using one-to-one domain mappings.

Configuring the Directory Information Tree

To configure the DIT:

1. Set a mapping rule in the Active Directory synchronization profile used for import operations. In this example, the mapping rule is:

   ```
   Domain Rule
   Cn=users, dc=us, cd=MyCompany, dc=comusers.us.MyCompany.com:
   users.us.MyCompany.com
   ```

   This mapping rule indicates that only the users container must be synchronized by using one-to-one domain mappings.

   The DNs of the user entries in both Microsoft Active Directory and Oracle Internet Directory are identical.

   If you choose to synchronize multiple subtrees, then you must configure multiple domain rules.

2. Set up the default realm, `usersearchbase`, and `groupsearchbase` values in Oracle Internet Directory. These values indicate to the various Oracle components where to look for users and groups in Oracle Internet Directory. During installation, be sure to set them correctly. Otherwise, even if the synchronization

seems to function properly, components still may not be able to access users and groups in Oracle Internet Directory.

The default realm is set up during installation However, if the default realm value is incorrectly specified during installation, then do the following:

- If Oracle Application Server has been installed but not yet deployed, then it is easier to re-install everything with the correct default realm value.
- If Oracle Application Server applications have already been deployed, then you must change the default realm.

The `usersearchbase` and `groupsearchbase` values refer to the roots of the subtrees in Oracle Internet Directory under which Oracle components look for users and groups. These values are set to default values during installation. However, in deployments requiring integration with Microsoft Active Directory, these values must be reset to the appropriate values, depending on the DIT structure in Active Directory.

For example, in the above example, the value of `usersearchbase` should be set to at least `cn=users,dc=us,dc=MyCompany,dc=com` or one of its parents. Similarly, the `groupsearchbase` can be set to `cn=groups,dc=us, dc=MyCompany,dc=com`, assuming that there is a subtree named `groups` in the DIT.

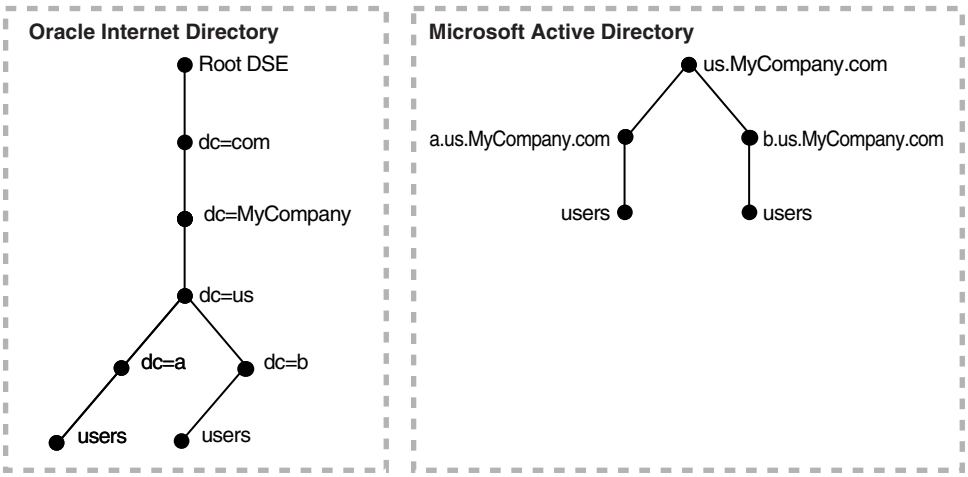
The `usersearchbase` and `groupsearchbase` values are set as part of Windows integration setup discussed in "Configuring the Active Directory Connector" on page 2-15.

The Directory Information Tree in a Multiple-Domain Active Directory Environment

Microsoft Active Directory deployment with multiple domains can have one single DIT or a forest of trees. In this typical scenario, Microsoft Active Directory has multiple domain controllers. A deployment with multiple domain controllers can have one single DIT or a forest of trees. The mapping between the DIT on Oracle Internet Directory and the DIT on Microsoft Active Directory for the single tree and the forest configurations are shown in Figure 2–2 and Figure 2–3, respectively.

Figure 2–2 shows an example of how multiple domains in Microsoft Active Directory are mapped to a DIT in Oracle Internet Directory.

Figure 2–2 Integration of Oracle Internet Directorywith Multiple Domains in Microsoft Active Directory

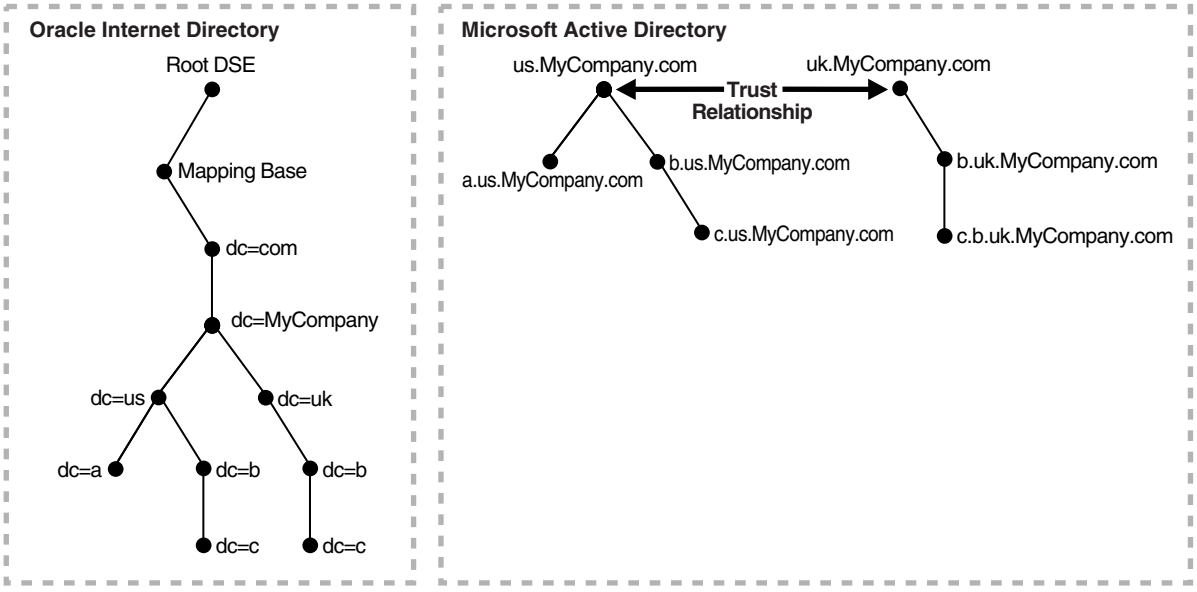


In Figure 2–2, the Microsoft Active Directory environment has a parent and two child domains. Each domain has a domain controller associated with it. The Microsoft Active Directory supporting the node `us.mycompany.com` is the Global Catalog Server.

The first child domain-namely, `a.us.MyCompany.com`—maps to `dc=a,dc=us,dc=MyCompany,dc=com` in Oracle Internet Directory. The second child domain—namely, `b.us.MyCompany.com`, maps to `dc=b,dc=us,dc=MyCompany,dc=com` in Oracle Internet Directory. The common domain component in Microsoft Active Directory environment—namely, `us.MyCompany.com`—maps to the default identity management realm in Oracle Internet Directory—namely, `dc=us,MyCompany,dc=com`.

Figure 2–3 shows how a forest in Microsoft Active Directory is reflected in Oracle Internet Directory.

Figure 2–3 Mapping Between Oracle Internet Directory and a Forest in Microsoft Active Directory



In Figure 2–3, Microsoft Active Directory is the enterprise directory. In this directory, two domain trees constitute a forest, and this forest maps to an identically structured subtree in Oracle Internet Directory.

Tools for Configuring the Active Directory Connector

To lists and describes the tools you use to set up and manage integration with Microsoft Active Directory.

Table 2–4 Tools for Setting Up and Managing Integration with Microsoft Active Directory

Tool	Description
`adprofilecfg.sh`	A shell script that provides an easy way of setting configuration information related to the Windows environment, such as the Microsoft Active Directory host and port information. This tool is useful only in simple scenarios and can be used only to configure information in default profiles. Note that this tool sets the information in all the three default profiles. When you run this tool, it creates the three default profiles, described earlier, from master default profiles and then modifies them with the information it takes as input from the user. Various setup tasks in the next section refer to this tool. This tool resides in `$ORACLE_HOME/ldap/odi/admin`.
Directory Integration and Provisioning Assistant	A command-line tool primarily for initial migration of data. It also enables you to manage synchronization profiles. You can use it to create new default profiles and set various attributes in those profiles. Various setup tasks in next section are refer to this tool. **See Also:** *Oracle Internet Directory Administrator's Guide*, Appendix A, "Syntax for LDIF and Command-Line Tools" for more details about using the Directory Integration and Provisioning Assistant
Oracle Internet Directory Self-Service Console	A Web-based GUI tool for use by administrators and end users. In a Windows integration setup, is primarily used to configure information to manage realms and the user group search bases. It is also used to create and manage users and groups. **See Also:** *Oracle Internet Directory Administrator's Guide*, Chapter 31, "Oracle Internet Directory Self-Service Console" for instructions about using this tool to manage realms and user and group search bases
Oracle Directory Manager	A standalone Java- based GUI tool for managing all data in Oracle Internet Directory. You can use it to: ■ Create and manage various synchronization profiles ■ Customize default profiles ■ Monitor synchronization profiles and synchronization status ■ Troubleshoot synchronization **See Also:** *Oracle Internet Directory Administrator's Guide*, Chapter 4, "Directory Administration Tools" for more details
Command-line tools	Such tools as `ldapmodify` and `ldapsearch` for managing synchronization profiles and troubleshooting. Various set up tasks in next section refer to these tools, too. Once you know the various setup requirements for Windows integration, these tools are very handy for quick customization. **See Also:** *Oracle Internet Directory Administrator's Guide*, Appendix A, "Syntax for LDIF and Command-Line Tools"

High-Level Configuration Requirements

There are two common ways of deploying integration with a Microsoft Windows environment. In the first, Oracle Internet Directory is the central enterprise directory and source of truth for user and group data for the Microsoft Windows 2000 and Windows NT environments. In the second, Microsoft Active Directory is the central enterprise directory and source of truth for user and group data for Oracle components.

This section contains these topics:

- Deployments with Oracle Internet Directory
- Deployments with Microsoft Active Directory as the Central Directory

Deployments with Oracle Internet Directory as the Central Directory

Table 2–5 describes the typical requirements in this deployment.

Table 2–5 Typical Requirements with Oracle Internet Directory as the Central Directory

Requirement	Oracle Internet Directory as Central
Initial bootstrapping	The Directory Integration and Provisioning Assistant populates Microsoft Active Directory with users and groups stored in Oracle Internet Directory. If there are multiple Microsoft Active Directory servers, then the Directory Integration and Provisioning Assistant must be run as many times as there are Microsoft Active Directory servers. Each time you do this, you choose the specific data set required by the target Microsoft Active Directory server.
Synchronization	User and group information is managed in Oracle Internet Directory. Changes to that information are synchronized with Microsoft Active Directory by the Oracle directory integration and provisioning server. The less likely synchronization from Microsoft Active Directory into Oracle Internet Directory can be achieved by configuring an import profile.
Passwords and password verifiers	Passwords are managed in Oracle Internet Directory by using such Oracle tools as the Oracle Internet Directory Self-Service Console. Password changes are synchronized with Microsoft Active Directory by the Oracle directory integration and provisioning server. However, before this server can synchronize the password changes, the password synchronization must be configured in the mapping rules. If the Oracle environment requires a password verifier, the latter is automatically generated when a new user entry is created or when a password is modified.
Oracle Application Server Single Sign-On	Once the OracleAS Single Sign-On server is configured, users log into the Oracle environment through it. When called upon by the OracleAS Single Sign-On server to authenticate a user, the Oracle directory server uses credentials available locally. No external authentication is involved. Users must log in only once to access various applications in the Oracle environment.
Windows native authentication (autologin)	This can be enabled for Windows-based users by configuring the OracleAS Single Sign-On server in the autologin mode. When Windows native authentication is configured, Windows users, once they login into the Windows desktop, need not log into the Oracle environment again.
Active Directory external authentication plug-in	Because user credentials are managed locally in Oracle Internet Directory, the Active Directory external authentication plug-in is not required.

New users or groups created in Oracle Internet Directory, are automatically provisioned into the Microsoft Windows environment by the Oracle directory integration and provisioning server. Before this provisioning can take place, a one-way synchronization must be configured between Oracle Internet Directory and Microsoft Active Directory.

If multiple Microsoft Active Directory servers are involved, then the Oracle directory integration and provisioning server provisions users and groups in the respective Microsoft Active Directory servers. Before this provisioning can take place, a one-way synchronization must be configured between Oracle Internet Directory and Microsoft Active Directory.

Deployments with Microsoft Active Directory as the Central Directory

Table 2–6 describes the typical requirements in this deployment.

Table 2–6 Typical Requirements with Microsoft Active Directory as the Central Directory

Requirement	Microsoft Active Directory as Central
Initial bootstrapping	The Directory Integration and Provisioning Assistant populates Oracle Internet Directory with users and groups stored in Microsoft Active Directory. If there are multiple Microsoft Active Directory servers, then the Directory Integration and Provisioning Assistant must be run as many times as there are Microsoft Active Directory servers. You can choose to manage user information, including password credentials, only in Microsoft Active Directory. In such deployments, to enable single sign-on in the Oracle environment, the Oracle directory integration and provisioning server can synchronize a minimal set of attributes of the user entry into Oracle Internet Directory. Passwords are not migrated.
Synchronization	The source of truth for user and group information is Microsoft Active Directory, and that information is managed there. Changes to user and group information are also synchronized by the Oracle directory integration and provisioning server from Microsoft Active Directory servers into Oracle Internet Directory. The less likely synchronization from Oracle Internet Directory to Microsoft Active Directory is achieved by configuring an export profile.
Passwords and password verifiers	It is assumed that passwords are managed in Microsoft Active Directory by using Microsoft Windows tools. The Oracle directory integration and provisioning server does not synchronize password changes into Oracle Internet Directory. In this deployment, it is not possible to generate password verifiers that the Oracle environment may require. To make a password verifier available in the Oracle environment, a user enables it to be generated by setting the password in the Oracle environment. However, in this case the Oracle directory server generates a password verifier when a password changes. It does not store the password in the `userpassword` attribute, which stays empty.
Oracle Application Server Single Sign-On	Once the OracleAS Single Sign-On server is configured, users log into the Oracle environment through it. To access various components in the Oracle environment, they must log in only once. Users with credentials only in Microsoft Active Directory are authenticated by the Oracle directory server invoking the external authentication plug-in. Users with credentials in Oracle Internet Directory are authenticated locally by the Oracle directory server.
Windows native authentication (autologin)	Same as in Oracle Internet Directory-centered deployment. However, for a user to use autologin, the user must exist in the Microsoft Active Directory. If Oracle Internet Directory contains some local users, then single sign-on does not function for them if Windows native authentication is enabled. Such users require that the attributes `orclsamaccountname` and `krbprincipalname` be populated in their user entries before single sign-on can function for them.
Active Directory external authentication plug-in	Because user credentials are managed in Microsoft Active Directory, this plug-in is required. When called upon by the OracleAS Single Sign-On server to authenticate a user, the Oracle directory server discovers that the credentials are not available in Oracle Internet Directory. It then invokes the external authentication plug-in. The plug-in performs the authentication of the user against the user credentials stored in Microsoft Active Directory.

New users or groups created in Microsoft Active Directory are automatically provisioned into Oracle Internet Directory by the Oracle directory integration and

provisioning server. Before the provisioning can take place, a one-way synchronization between Microsoft Active Directory and Oracle Internet Directory must be established.

If multiple Microsoft Active Directory servers are involved, then the Oracle directory integration and provisioning server provisions users and groups from the respective Microsoft Active Directory servers into Oracle Internet Directory. Before the provisioning can take place, a one-way synchronization between Oracle Internet Directory and each Microsoft Active Directory server must be established.

Passwords are not migrated.

Planning the Integration with Microsoft Active Directory

To successfully set up the integration of Oracle Identity Management with Microsoft Active Directory, do the following:

- Determine the kind of synchronization required. You base this determination on:
  - Whether Oracle Internet Directory or Microsoft Active Directory is to be the source of truth for user and group information
  - Whether one-way or two-way synchronization is required
  - Whether single or multiple Microsoft Active Directory domains are to be integrated
  - In case of multiple domains, whether the Global Catalog is configured in the Microsoft Active Directory environment.
- Determine whether the Active Directory external authentication plug-in is required. If it is, then follow the steps in "Configuring the Active Directory Connector" on page 2-15.
- If you are synchronizing from Microsoft Active Directory to Oracle Internet Directory, and need to track changes in Microsoft Active Directory, then determine the tracking approach by using Table 2–2 on page 2-4. The synchronization scenarios described later in "Configuring the Active Directory Connector" on page 2-15 are based on the USNChanged approach. However, to use the DirSync approach, the synchronization scenarios requires a minor change that is documented in the scenarios.
- If the synchronization scenarios described in section "Configuring the Active Directory Connector" on page 2-15 do not meet your requirements, then see "Customizing the Active Directory Connector" on page 2-32.

Once you are ready for synchronization, but before you start it, decide whether you need initial migration of data from Microsoft Active Directory to Oracle Internet Directory or from Oracle Internet Directory to Microsoft Active Directory. If you do, then follow the steps in the "Migrating Data Between Directories" on page 2-37.

> **See Also:** "Configuring the Active Directory Connector" on page 2-15 for instructions for setting up various synchronization scenarios

Configuring the Active Directory Connector

This section explains how to configure integration with Microsoft Active Directory in various scenarios.

This section contains these topics:

Summary of Active Directory Connector Configuration Scenarios

The scenarios described in this section share these assumptions:

- The default set of attributes installed with Oracle Internet Directory are sufficient for synchronization
- Only user and group objects must be synchronized
- Migration of users and groups from Microsoft Active Directory is not required

Synchronization Scenarios with Single-Domain Microsoft Active Directory Environments

Table 2–7 Scenarios with Single-Domain Microsoft Active Directory Environments

Scenario#	Synchronization Configuration
Scenario1	Users and groups from Microsoft Active Directory to Oracle Internet Directory
Scenario2	Users and groups from Oracle Internet Directory to Microsoft Active Directory
Scenario3	Two-way synchronization of users and groups between Oracle Internet Directory and Microsoft Active Directory

Synchronization Scenarios with Multiple-Domain Microsoft Active Directory Environments

Table 2–8 Scenarios with Multiple-Domain Microsoft Active Directory Environments

Scenario#	Synchronization Configuration
Scenario4	Users and groups from Global Catalog Server to Oracle Internet Directory
Scenario5	Users and groups from Microsoft Active Directory to Oracle Internet Directory without a Global Catalog Server
Scenario6	Users and Groups from Oracle Internet Directory to Microsoft Active Directory

About Scenario Examples

Each scenario in this section uses an example. These examples rest on the following assumptions:

- The synchronization of users and groups between Oracle Internet Directory and Microsoft Active Directory always use one-to-one domain mapping—that is, the DN of the user and group entries are the same in both directories.
- Oracle Internet Directory is installed on a host `iasdemo.us.mycompany.com`. This means that the default realm of Oracle Internet Directory is `dc=us,dc=mycompany,dc=com`.
- The Oracle directory server is running on port 389.
- The password for the directory administrator, as chosen during installation of Oracle Internet Directory, was `welcome1`.
- Other tools, namely, the Directory Integration and Provisioning Assistant and `adprofilecfg.sh` prompt you for a password. The password you should supply is `welcome1`.
- The `adprofilecfg.sh` prompts you for a super user DN. The value you should supply is `dn=orcladmin`.
- In a single-domain Microsoft Active Directory environment, the host name is `addemo.us.mycompany.com`. This means that the domain of the Microsoft Active Directory host is the same as the default realm of Oracle Internet Directory as set during installation, namely, `dc=us,dc=mycompany,dc=com`.

  If this is not true, then, during installation of Oracle Internet Directory, the default realm value must be set to correspond to the Microsoft Active Directory domain. In this example, that domain is `dc=us,dc=mycompany,dc=com`.

  If you have already installed Oracle Internet Directory and the default realm does not correspond to the domain of the Microsoft Active Directory host, then Oracle Corporation recommends that you re-install the Oracle Identity Management. As you do this, set the proper value of default realm, otherwise the setup scenarios described in this section fail.
- In this section, the examples of multiple-domain Microsoft Active Directory environments use two domains having the host names `ad1demo.a.us.mycompany.com` and `ad2demo.b.us.mycompany.com`. This means that the domains of Microsoft Active Directory hosts are respectively `dc=a,dc=us,dc=mycompany,dc=com` and `dc=b,dc=us,dc=mycompany,dc=com`.

  Further, during installation of Oracle Internet Directory, the default realm value must be set to the parent of the Microsoft Active Directory server domains. In this example, the default realm value is `dc=us,dc=mycompany,dc=com`. If this is not true, then Oracle Corporation recommends that you re-install Oracle Identity Management. As you do this, set the proper value of default realm, otherwise the setup scenarios described in this section fail.
- The scenario described later uses the USNChanged approach for tracking changes in Active Directory. However, if the user wishes to use the DirSync approach, replace the profile `ActiveChgImp` with the profile `activeImport` Tasks 1-5 required in this setup.
- Every user created from Oracle Internet Directory requires an object class `orclADUser` to be added the entry, which has a mandatory attribute of `orclSAMAccountName`. Note that, `orclSAMAccountName` cannot have any special characters in it. If you are creating users from Oracle Internet Directory Self-Service Console, then you need to modify the user creation property through the Console to include the `orclADUser` object class and `orclSAMAccountName`.

Further, the value of the attribute `orclSAMAccountName` could be given as `ActiveDirectorydomain$userid`.

About the Information You Must Add to the Active Directory Connector

Most of the configuration information required for enabling synchronization is preconfigured in Oracle Internet Directory during installation. Beyond that preconfigured information, you need to add a minimal amount of information to the Active Directory connector.

The information you must add to the Active Directory connector pertains to the Microsoft Active Directory environment. This information includes:

- Microsoft Active Directory URL (`host:port`)
- Microsoft Active Directory user account and password to be used by the Active Directory connector
- Microsoft Active Directory domain containing the users and groups to be synchronized

To add this information, you can use either command-line tools or Oracle Directory Manager.

Moreover, if the default realm is changed, then you must re-create the ACLs to enable only the owners of various synchronization profiles to create, modify, and delete entries under the user and group containers. Although default ACLs are created during installation, most often they must be modified to meet the security needs of the deployment. The section "Scenario 1: One-Way Synchronization from Microsoft Active Directory to Oracle Internet Directory" on page 2-20 advises you as to when you need to change an ACL.

> **See Also:** *Oracle Internet Directory Administrator's Guide*, Chapter 3, "Preliminary Tasks and Information" for more information about customizing the default access control configuration

About the adprofilecfg.sh Tool

The scenarios described in the next sections use the `adprofilecfg.sh` tool to configure Microsoft Active Directory-related information into the default profiles. This tool creates three default profiles from master default profiles and then modifies them with the information it receives from the user. If you have already customized one of the default profiles, then the `adprofilecfg.sh` tool overwrites it. In this case, rename your default profile as described in the next section, "Tasks Common to Various Scenarios".

Tasks Common to Various Scenarios

This section discusses tasks that, in most scenarios, you must perform only once for a given installation. For example, suppose that you are following both Scenario 1 and Scenario 2 described later in this chapter. If, you perform these tasks to set up Scenario 1, then you do not need to perform them again to set up Scenario 2.

Task 1: Verify the Microsoft Active Directory Information to be Configured into the Active Directory Synchronization Profiles

To do this, enter the following command against the Microsoft Active Directory server:

```
ldapsearch -p port -h host -D user account -w password -b "" -s base
"objectclass=*" defaultnamingcontext
```

For example:

```
ldapsearch -p 389 -h adtest.us.MyCompany.com -D Administrator@us.MyCompany.com -w
welcome1 -b "" -s base "objectclass=*" defaultnamingcontext
```

This should return the domain name of the Microsoft Active Directory server. In our example, the exact output should be:

```
defaultNamingContext=DC=us,DC=MyCompany,dc=com
```

Task 2: Configure the Information Related to the Microsoft Active Directory Environment

This includes adding to the synchronization profile used for synchronization the information explained in "Information Required During Setup" on page 2-7.

If you are using the default synchronization profiles, then run the script `$ORACLE_HOME/ldap/odi/admin/adprofilecfg.sh` to set up the information. The script prompts you for the following:

- The Oracle Internet Directory super user DN and password
- The Microsoft Active Directory URL (host:port)
- The Microsoft Active Directory user account and password to be used by the Active Directory connector
- The Microsoft Active Directory domain to be synchronized-for example, `cn=users,dc=us,dc=com`.

Once you have entered the parameter values, `adprofilecfg.sh` invokes the Directory Integration and Provisioning Assistant. The Assistant sets up the Microsoft Active Directory connection information and mapping rules information in the default Active Directory synchronization profiles.

Note: This step is required only once for all the synchronization scenarios where default profiles are used.

Task 3: Start the Oracle Directory Integration and Provisioning Server as You Would for Synchronization

---

Note:

- This step is required only once to start the directory integration and provisioning server for the synchronization. However, the synchronization does not start until a synchronization profile is enabled.
- A directory integration and provisioning server is always running by default after installation as `instance=1`. That directory integration and provisioning server is unrelated to the one required for synchronization. The directory integration and provisioning server used for synchronization must run as an instance greater than `1`.

To start the directory integration and provisioning server as you would for synchronization, enter the following command:

```
oidctl connect=iasdb server=odisrv instance=2 configset=1 flags="port=3060" start
```

Synchronization Between a Single-Domain Microsoft Active Directory and Oracle Internet Directory

This section describes various scenarios for setting up one-way synchronization of users and groups between a single-domain Microsoft Active Directory and Oracle Internet Directory.

Scenario 1: One-Way Synchronization from Microsoft Active Directory to Oracle Internet Directory

This scenario rests on these assumptions:

- Only the default set of attributes must be synchronized from Microsoft Active Directory to Oracle Internet Directory.
- No initial migration of data is required, as is typical for demo and test systems.

In general, to set up this scenario, do the following:

1. Perform Tasks 1 through 3 described in "Tasks Common to Various Scenarios" on page 2-18.
2. If you are synchronizing groups, then perform Tasks 4 through 6 as described in this section.

Task 4: (Required only if you are synchronizing groups) Configure ACLs for Group Synchronization

> **Note:** This step is required only if groups are being synchronized.

This task sets up the proper access controls to enable groups to be created under the `users` container. To set up the proper access controls, do this:

1. Create an LDIF file named `grantrole.ldif`. The sample file is given at the end of this chapter. If the default realm is not `dc=us,dc=mycompany,dc=com`, then edit the file `grantrole.ldif` and replace every `dc=us,dc=mycompany,dc=com` string with the actual default realm—for example, `dc=us,dc=YourCompany,dc=com`. Save the file.
2. Enter the command:

   ```
   ldapmodify -h host -p port -D DN of orcladmin -p password -f grantrole.ldif
   ```

   For example,

   ```
   ldapmodify -c -h iasdemo -p 3060 -D cn=orcladmin -w welcome1 -f grantrole.ldif
   ```

   This configures the required ACL policy in Oracle Internet Directory to enable creation and modification of groups in Oracle Internet Directory.

Task 5: Start the Synchronization from Microsoft Active Directory to Oracle Internet Directory

This requires enabling the respective profile by setting the `profileStatus` attribute to `ENABLE`. To do this, enter the command:

```
Dipassistant mp -profile ActiveChgImp odip.profile.status = ENABLE
```

Task 6: Verify that Synchronization Has Started

Enter the following command:

```
ldapsearch -h oid_host -p oid_port -D cn=dipadmin -w orcladmin_password -b
"orclodipagentname=activechgimp,cn=subscriber profile,cn=changelog
subscriber,cn=oracle internet directory' -s base "objectclass=*"
orclodipsynchronizationstatus orclodiplastsuccessfulexecutiontime
```

Table 2–9 shows the values of the status attributes when synchronization is successfully started.

Table 2–9 Attribute Values Indicating Successful Synchronization

Attribute	Value Indicating Successful Synchronization
Synchronization Status	Synchronization successful
Last Successful Execution Time	*Date and time* (**Note:** This must be close to the current date and time.)

An example of a result indicating successful synchronization is:

```
Synchronization successful November 04, 2003 15:56:03
```

Notes:

- The date and time must be close to current date and time.
- When running the `ldapsearch` command, you need the `dipadmin` password, which, as established at installation, is the same as `orcladmin` password.

Scenario 2: One-Way Synchronization from Oracle Internet Directory to Microsoft Active Directory

This scenario rests on the same assumptions as those in "Scenario 1: One-Way Synchronization from Microsoft Active Directory to Oracle Internet Directory" on page 2-20, but the synchronization is from Oracle Internet Directory to Microsoft Active Directory. This scenario does not require you to set up any additional information, nor does it require you to set up access controls.

In general, to set up this scenario, do the following:

1. Perform Tasks 1 through 3 described in "Tasks Common to Various Scenarios" on page 2-18.
2. Perform Tasks 4 and 5 as described in this section.

Task 4: Start the Synchronization from Microsoft Active Directory to Oracle Internet Directory

This requires enabling the respective profile by setting the `profileStatus` attribute to `ENABLE`. To do this, enter the command:

```
Dipassistant mp -profile ActiveChgImp odip.profile.status = ENABLE
```

Task 5: Verify that Synchronization Has Started

Enter the following command:

```
ldapsearch -h oid_host -p oid_port -D cn=dipadmin -w orcladmin_password -b
"orclodipagentname=activechgimp,cn=subscriber profile,cn=changelog
subscriber,cn=oracle internet directory' -s base "objectclass=*"
orclodipsynchronizationstatus orclodiplastsuccessfulexecutiontime
```

Table 2–10 shows the values of the status attributes when synchronization is successfully started.

Table 2–10 Attribute Values Indicating Successful Synchronization

Attribute	Value Indicating Successful Synchronization
Synchronization Status	Synchronization successful
Last Successful Execution Time	*Date and time* (**Note:** This must be close to the current date and time.)

An example of a result indicating successful synchronization is:

```
Synchronization successful November 04, 2003 15:56:03
```

Notes:

- The date and time must be close to current date and time.
- When running the `ldapsearch` command, you need the `dipadmin` password, which, as established at installation, is the same as `orcladmin` password.

Scenario 3: Two-Way Synchronization Between Oracle Internet Directory and Microsoft Active Directory

To set up two-way synchronization, execute both Scenario 1 and Scenario 2 as previously described.

Synchronization Between a Multiple-Domain Microsoft Active Directory and Oracle Internet Directory

This section describes setup tasks for a two-domain Microsoft Active Directory environment. In a Microsoft Active Directory environment with more than two domains, the tasks for setting up synchronization for additional domains are similar to those outlined in this section.

Scenario 4: One-Way Synchronization from Microsoft Active Directory to Oracle Internet Directory when Global Catalog Is Configured in the Microsoft Active Directory Environment

Note: The Global Catalog can be used only for synchronizing changes from Microsoft Active Directory to Oracle Internet Directory. Further, it can be used only when the USNChanged method is used to track changes in Microsoft Active Directory.

To illustrate this scenario, we use a sample deployment with two Microsoft Active Directory domain servers:

- `a.us.MyCompany.com`

- `b.us.MyCompany.com`

If there are more than two domains, then the setup procedures are the same as those in Scenario 1, with the exception of Task 4 in which the LDIF file is customized to the actual multiple-domain environment.

In general, to set up this scenario, do the following:

1. Perform Tasks 1through 3 as described in "Tasks Common to Various Scenarios" on page 2-18.
2. Perform Tasks 4 through 6 as described in this section.

As you perform Tasks 1 through 3, keep these considerations in mind:

- In Tasks 1 and 2, make sure that the Microsoft Active Directory host and port information are those where the Global Catalog is running. The default port number on which global catalog is running is 3268.
- In Task 2, you must properly supply the value of the Microsoft Active Directory domain. Usually it should be the DN of the entry that is the parent of all the Microsoft Active Directory domains. In our example, this value should be `dc=us,dc=MyCompany,dc=com`.

Task 4: Create the Appropriate DIT Structure and Configure Required ACLs for User and Group Synchronization

Oracle Internet Directory does not have the complete DIT structure ready for use in a multiple-domain Microsoft Active Directory scenario. It requires performing the following:

- Creating some entries in Oracle Internet Directory. In our example, to create the users container for the first domain, it requires creating entries with following DNs:

  ```
  dc=a,dc=us,dc=mycompany,dc=com
  dc=b,dc=us,dc=mycompany,dc=com
  cn=users,dc=a,dc=us,dc=mycompany,dc=com
  ```

  To create the users container for the second domain requires creating entries with following DN:

  ```
  cn=users,dc=b,dc=us,dc=mycompany,dc=com
  ```

- Assigning ACLs to the `users` containers to allow users and groups to be created under those containers

  Reset the User Search Base and Group Search Base to point to the value `dc=us,dc=mycompany,dc=com`. This allows all Oracle applications to be able to find users and groups in the two `users` containers.

- Creating an LDIF file by named `multidomaindit.ldif`. This file creates the appropriate DIT structure and the required ACLs for our example.
- You can see an example of this file in "multidomaindit.ldif" on page 2-44. You can edit this file by replacing sample Microsoft Active Directory domains in this scenario with those in your environment.

  To load this file, enter the following command:

  ```
  ldapmodify -h host -p port -D DN of orcladmin -p password -f
  multidomaindit.ldif
  ```

  For example:

```
ldapmodify -h iasdemo -p 3060 -D cn=orcladmin -p welcome1 -f
multidomaindit.ldif
```

Task 5: Start the Synchronization from Microsoft Active Directory to Oracle Internet Directory

This requires enabling the respective profile by setting the `profileStatus` attribute to `ENABLE`. To do this, enter the following command:

```
Dipassistant mp -profile ActiveChgImp odip.profile.status = ENABLE
```

Task 6: Verify that Synchronization Has Started

Enter the following command:

```
ldapsearch -h oid_host -p oid_port -D cn=dipadmin -w orcladmin_password -b
"orclodipagentname=activechgimp,cn=subscriber profile,cn=changelog
subscriber,cn=oracle internet directory' -s base "objectclass=*"
orclodipsynchronizationstatus orclodiplastsuccessfulexecutiontime
```

A shows the values of the status attributes when synchronization is successfully started.

Table 2–11 Attribute Values Indicating Successful Synchronization

Attribute	Value Indicating Successful Synchronization
Synchronization Status	Synchronization successful
Last Successful Execution Time	*Date and time* (**Note:** This must be close to the current date and time.)

An example of a result indicating successful synchronization is:

```
Synchronization successful November 04, 2003 15:56:03
```

Notes:

- The date and time must be close to current date and time.
- When running the `ldapsearch` command, you need the `dipadmin` password, which, as established at installation, is the same as `orcladmin` password.

Scenario 5: One-Way Synchronization from Microsoft Active Directory to Oracle Internet Directory when Global Catalog is not Configured in the Microsoft Active Directory Environment

Notes:

- If there are more than two domains, then the setup procedure outlined in this section is same except Task 4 where the LDIF file must be modified to suit the actual multiple-domain environment.
- This setup requires the creation of as many profiles as there are Microsoft Active Directory domains. In our example, the setup requires two profiles. This scenario makes use of the one default profile, namely, `ActiveChgImp`, renaming it to `ActiveChgImp1` and then creating another profile named `ActiveChgImp`.

In general, to set up this scenario, do the following:

1. On the first Microsoft Active Directory domain, perform Tasks 1 through 3 as described in "Tasks Common to Various Scenarios" on page 2-18. You can call this domain, for example, `a.MyOracle.com`.
2. Perform Tasks 4 through 9 as described in this section.

As you perform Tasks 1 through 3, keep the following in mind:

- In Tasks 1 and 2, make sure that the Microsoft Active Directory host and port information is that of first domain server. In our example, this is `a.MyOracle.com`.
- In Task 2, the value of the Microsoft Active Directory domain must be properly supplied. Usually, this is the DN of the Microsoft Active Directory domain entry. In our example, this value is `dc=a,dc=us,dc=MyCompany,dc=com`.

Task 4: Create the Appropriate DIT Structure and Configure Required ACLs for User and Group Synchronization

Oracle Internet Directory does not have the complete DIT structure ready for use in a multiple-domain Microsoft Active Directory scenario. It requires performing the following:

- Creating some entries in Oracle Internet Directory. In our example, to create the users container for the first domain, it requires creating entries with following DNs:

  ```
  dc=a,dc=us,dc=mycompany,dc=com
  dc=b,dc=us,dc=mycompany,dc=com
  cn=users,dc=a,dc=us,dc=mycompany,dc=com
  ```

  To create the users container for the second domain requires creating entries with following DN:

  ```
  cn=users,dc=b,dc=us,dc=mycompany,dc=com
  ```

- Assigning ACLs to the `users` containers to allow users and groups to be created under those containers

  Reset the *User Search Base* and *Group Search Base* to point to the value `dc=us,dc=mycompany,dc=com`. This allows all Oracle applications to be able to find users and groups in the two `users` containers.

- Creating an LDIF file by named `multidomainditimp.ldif`. This file creates the appropriate DIT structure and the required ACLs for our example.

  You can find an example of this file at "multidomaindit.ldif" on page 2-44.

  To load this file, enter the following command:

  ```
  ldapmodify -h host -p port -D DN of orcladmin -p password -f
  multidomaindit.ldif
  ```

  For example:

  ```
  ldapmodify -h iasdemo -p 3060 -D cn=orcladmin -p welcome1 -f
  multidomaindit.ldif
  ```

Task 5: Rename a Profile

Renaming a profile requires:

- Adding permissions for it in the directory. The permissions allow the directory integration and provisioning server to add, modify, and delete users and groups on behalf of the connector using the renamed profile.
- Removing permissions for the old profile

For example, using the sample file in the section "renameprofile.ldif" on page 2-46, create a profile with the name `renameprofile.ldif`. The sample profile assumes that you are renaming a default import profile from `ActiveChgImp` to `ActiveChgImp1`. Do the following:

1. Modify the LDIF file to replace the names `ActiveChgImp` and `ActiveChgImp1` with your profile names.
2. Enter the following command:

   ```
   ldapmodify -h host -p port -D DN of orcladmin -p password -f renameprofile.ldif
   ```

   For example:

   ```
   ldapmodify -h iasdemo -p 3060 -D cn=orcladmin -p welcome1 -f renameprofile.ldif
   ```

Task 6: Create Another Profile for the Second Microsoft Active Directory Domain Server (b.MyCompany.com)

To do this, enter the following command:

```
Dipassistant cp $ORACLE_HOME/ldap/odi/conf/activechgimp.properties
```

This creates another profile named `ActiveChgImp`.

Task 7: On the New Profile, Perform Tasks 1 and 2

On the second directory domain, namely, `b.MyOracle.com`, perform Tasks 1 and 2 as described in "Tasks Common to Various Scenarios" on page 2-18. Keep the following in mind:

- In Tasks 1 and 2, make sure that the Microsoft Active Directory host and port information is that of second domain server. In our example, this is `b.MyOracle.com`.
- In Task 2, the value of the Microsoft Active Directory domain must be properly supplied. Usually, it should be the DN of the Microsoft Active Directory domain entry. In the example described above, this value should be `dc=b,dc=us,dc=MyCompany,dc=com`.

Task 8: Start the Synchronization from Microsoft Active Directory to Oracle Internet Directory

This requires enabling the respective profile by setting the `profileStatus` attribute to `ENABLE`.

To start the synchronization enter the command:

```
Dipassistant mp -profile ActiveChgImp odip.profile.status = ENABLE
Dipassistant mp -profile ActiveChgImp1 odip.profile.status = ENABLE
```

This starts the synchronization from both Microsoft Active Directory domains to Oracle Internet Directory.

Task 9: Verify that Synchronization Has Started

Enter the following command:

```
ldapsearch -h oid_host -p oid_port -D cn=dipadmin -w orcladmin_password -b
```

```
"orclodipagentname=activechgimp,cn=subscriber profile,cn=changelog
subscriber,cn=oracle internet directory' -s base "objectclass=*"
orclodipsynchronizationstatus orclodiplastsuccessfulexecutiontime
```

Table 2–12 shows the values of the status attributes when synchronization is successfully started.

Table 2–12 Attribute Values Indicating Successful Synchronization

Attribute	Value Indicating Successful Synchronization
Synchronization Status	Synchronization successful
Last Successful Execution Time	*Date and time* (**Note:** This must be close to the current date and time.)

An example of a result indicating successful synchronization is:

```
Synchronization successful November 04, 2003 15:56:03
```

Notes:

- The date and time must be close to current date and time.
- When running the `ldapsearch` command, you need the `dipadmin` password, which, as established at installation, is the same as `orcladmin` password.

Scenario 6: One-Way Synchronization from Oracle Internet Directory to Microsoft Active Directory

Notes:

- If there are more than two domains, then the setup procedure outlined in this section is the same, except Task 4 where the LDIF file must be modified to suit the actual multiple-domain environment.
- This setup requires the creation of as many profiles as there are Microsoft Active Directory domains. In our example, the setup requires two profiles. This scenario makes use of the one default profile, namely, `ActiveExport`, renaming it to `ActiveExport1` and then creating another profile named `ActiveExport`.

In general, to set up this scenario, do the following:

1. On the first Microsoft Active Directory domain, perform Tasks 1 through 3 as described in "Tasks Common to Various Scenarios" on page 2-18. You can call this domain, for example, `a.MyOracle.com`.
2. Perform Tasks 4 through 9 as described in this section.

As you perform Tasks 1 through 3, keep the following in mind:

- In Tasks 1 and 2, make sure that the Microsoft Active Directory host and port information is that of first domain server. In our example, this is `a.MyOracle.com`.

- In Task 2, the value of the Microsoft Active Directory domain must be properly supplied. Usually, this is the DN of the Microsoft Active Directory domain entry. In our example, this value is `dc=a,dc=us,dc=MyCompany,dc=com`.

Task 4: Create the Appropriate DIT Structure and Configure Required ACLs for User and Group Synchronization

Oracle Internet Directory does not have the complete DIT structure ready for use in a multiple-domain Microsoft Active Directory scenario. It requires performing the following:

- Creating some entries in Oracle Internet Directory. In our example, to create the users container for the first domain, it requires creating entries with following DNs:

  ```
  dc=a,dc=us,dc=mycompany,dc=com
  dc=b,dc=us,dc=mycompany,dc=com
  cn=users,dc=a,dc=us,dc=mycompany,dc=com
  ```

  To create the users container for the second domain requires creating entries with following DN:

  ```
  cn=users,dc=b,dc=us,dc=mycompany,dc=com
  ```

- Assigning ACLs to the `users` containers to allow users and groups to be created under those containers

  Reset the *User Search Base* and *Group Search Base* to point to the value `dc=us,dc=mycompany,dc=com`. This allows all Oracle applications to be able to find users and groups in the two `users` containers.

- Creating an LDIF file by named `multidomainditimp.ldif`. This file creates the appropriate DIT structure and the required ACLs for our example.

  You can find an example of this file at "multidomaindit.ldif" on page 2-44.

  To load this file, enter the following command:

  ```
  ldapmodify -h host -p port -D DN of orcladmin -p password -f
  multidomaindit.ldif
  ```

  For example:

  ```
  ldapmodify -h iasdemo -p 3060 -D cn=orcladmin -p welcome1 -f
  multidomaindit.ldif
  ```

Task 5: Rename a Profile

Renaming a profile requires:

- Adding permissions for it in the directory. The permissions allow the directory integration and provisioning server to add, modify, and delete users and groups on behalf of the connector using the renamed profile.
- Removing permissions for the old profile

For example, using the sample file in the section "renameprofile.ldif" on page 2-46, create a profile with the name `renameprofile.ldif`. The sample profile assumes that you are renaming a default export profile from `ActiveExport` to `ActiveExport1`. Do the following:

1. Modify the LDIF file to replace the names `ActiveChgImp` to `ActiveExport` and `ActiveChgImp1` to `ActiveExport1`.

2. Enter the following command:

```
ldapmodify -h host -p port -D DN of orcladmin -p password -f renameprofile.ldif
```

For example:

```
ldapmodify -h iasdemo -p 3060 -D cn=orcladmin -p welcome1 -f renameprofile.ldif
```

Task 6: Create Another Profile for the Second Microsoft Active Directory Domain Server (b.MyCompany.com)

To do this, enter the following command:

```
Dipassistant cp $ORACLE_HOME/ldap/odi/conf/activeexport.properties
```

This creates another profile named `ActiveExport`.

Task 7: On the New Profile, Perform Tasks 1 and 2

On the second directory domain, namely, `b.MyOracle.com`, perform Tasks 1 and 2 as described in "Tasks Common to Various Scenarios" on page 2-18. Keep the following in mind:

- In Tasks 1 and 2, make sure that the Microsoft Active Directory host and port information is that of second domain server. In our example, this is `b.MyOracle.com`.
- In Task 2, the value of the Microsoft Active Directory domain must be properly supplied. Usually, it should be the DN of the Microsoft Active Directory domain entry. In the example described above, this value should be `dc=b,dc=us,dc=MyCompany,dc=com`.

Task 8: Start the Synchronization from Microsoft Active Directory to Oracle Internet Directory

This requires enabling the respective profile by setting the `profileStatus` attribute to `ENABLE`.

To start the synchronization enter the command:

```
Dipassistant mp -profile ActiveExport odip.profile.status = ENABLE
Dipassistant mp -profile ActiveExport1 odip.profile.status = ENABLE
```

This starts the synchronization from both Microsoft Active Directory domains to Oracle Internet Directory.

Task 9: Verify that Synchronization Has Started

Enter the following command:

```
ldapsearch -h oid_host -p oid_port -D cn=dipadmin -w orcladmin_password -b
"orclodipagentname=ActiveExport,cn=subscriber profile,cn=changelog
subscriber,cn=oracle internet directory' -s base "objectclass=*"
orclodipsynchronizationstatus orclodiplastsuccessfulexecutiontime
```

Table 2–13 shows the values of the status attributes when synchronization is successfully started.

Table 2–13 Attribute Values Indicating Successful Synchronization

Attribute	Value Indicating Successful Synchronization
Synchronization Status	Synchronization successful

Table 2–13 (Cont.) Attribute Values Indicating Successful Synchronization

Attribute	Value Indicating Successful Synchronization
Last Successful Execution Time	*Date and time* (Note: This must be close to the current date and time.)

An example of a result indicating successful synchronization is:

```
Synchronization successful November 04, 2003 15:56:03
```

Notes:

- The date and time must be close to current date and time.
- When running the `ldapsearch` command, you need the `dipadmin` password, which, as established at installation, is the same as `orcladmin` password.

Configuring The Active Directory External Authentication Plug-in

If you are storing passwords in Microsoft Active Directory, then you must use the Active Directory external authentication plug-in to authenticate Microsoft Active Directory users from Oracle Internet Directory.

This section tells how to install and enable the Active Directory external authentication plug-in.

For the most part, these instructions are the same for setting up the plug-in both single-domain and multiple-domain Microsoft Active Directory environments. There is, however, one difference: In a multiple-domain environment, the external authentication plug-in requires the Microsoft Active Directory Global Catalog Server.

This section contains these topics:

- Installing Active Directory External Authentication Plug-ins
- Enabling the Active Directory External Authentication Plug-ins

Installing Active Directory External Authentication Plug-ins

To install the plug-in:

1. Execute `$ORACLE_HOME/ldap/admin/oidspadi.sh`.

Note: To run shell script tools on the Windows operating system, you need one of the following UNIX emulation utilities:

- Cygwin 1.3.2.2-1 or later. Visit: `http://sources.redhat.com`
- MKS Toolkit 6.1. Visit: `http://www.datafocus.com/`

To execute `oidspadi.sh`, enter:

```
cd $ORACLE_HOME/ldap/admin
sh oidspadi.sh
```

If you are using the Windows operating system, then execute oidspadi.sh after you have installed the UNIX emulation utility by entering:

```
sh oidspadi.sh
```

2. Enter the Microsoft Active Directory host name. This is the Microsoft Active Directory to which you are going to synchronize. This value is required.
3. Enter the Microsoft Active Directory port number. In a multiple domain environment, the default port can be that of the global catalog server, namely, 3268.
4. Enter directory server host name. This value is required.
5. Enter directory server port number. The default port is 389.
6. Enter the password of the Oracle administrator (`orcladmin`). This value is required.
7. Enter the distinguished name of the container to which the plug-in needs to be applied. Every entry in this container will be authenticated against Microsoft Active Directory. Note that this need not necessarily be the User Search Base supplied in Oracle Internet Directory Self-Service Console. All the users under this search base are authenticated externally to the Microsoft Active Directory. If more than one container is specified, then separate the DNs with semi-colons (`;`).
8. Enter the value of the entry that is to be excluded from authentication to Microsoft Active Directory. This value is the exception to Step 7 the distinguished name of the container to which the plug-in needs to be ap. You need to enter the value in the standard `ldapsearch` filter format. For example, if you specify the value `(&(objectclass=inetorgperson)(cn=orcladmin))`, then any entry under the user container specified in Step 7 that has the `cn=orcladmin` and `objectclass=inetorgperson` attribute values will not be authenticated to Microsoft Active Directory.
9. Enter the Plug-in Request Group DN. For security reasons, the plug-in can be invoked only by users belonging to this group. For example, suppose that the Oracle Application Server Single Sign-On administrators are in the group `cn=OracleUserSecurityAdmins,cn=Groups,cn=OracleContext`. If you enter this DN as the vale for the Plug-in Request Group DN, then only requests coming from members of the Oracle Application Server Single Sign-On administrators can trigger the external authentication plug-in. You can enter multiple DN values. Use a semicolon (`;`) to separate them. This value is not required, but, for security purposes, it should be specified.
10. Enter the choice of using SSL connection to Active Directory or not. If you choose to use SSL, then you need to enter the following:
    a. The Active Directory SSL connection port number.
    b. The location of the Oracle wallet. This wallet needs to have the valid certificate from the Active Directory that you are trying to connect to.
    c. The Oracle wallet password.

    When specifying the wallet location on the Microsoft Windows operating system, add an additional backslash (`\`). For example, if the wallet location is `D:storage\wallet`, then enter `D:\\storage\\wallet`.
11. Specify the backup Microsoft Active Directory domain controller details (optional).

Enabling the Active Directory External Authentication Plug-ins

To enable the Active Directory external authentication plug-ins, use these two commands:

```
ldapmodify -h host -p port -D cn=orcladmin -w password <<EOF
dn: cn=adwhencompare,cn=plugin,cn=subconfigsubentry
changetype: modify
replace: orclpluginenable
orclpluginenable: 1
EOF

ldapmodify -h host -p port -D cn=orcladmin -w password <<EOF
dn: cn=adwhenbind,cn=plugin,cn=subconfigsubentry
changetype: modify
replace: orclpluginenable
orclpluginenable: 1
EOF
```

See Also: "Managing the Active Directory External Authentication Plug-in" on page 2-38

Customizing the Active Directory Connector

The section "Configuring the Active Directory Connector" on page 2-15 describes how to configure the Active Directory connector in a simple deployment that requires minimal configurations beyond the default ones. However, your deployment may be more complex and require you to customize the connector configurations.

Note: Be sure that your `ORACLE_HOME` is set to the correct value, otherwise the commands specified in various scenarios do not function properly.

This section describes various customizations a deployment may require. It contains these topics:

- Creating and Customizing a Synchronization Profile
- Customizing Mapping Rules
- Customizing the Search Filter to Get Information from Microsoft Active Directory
- Running the Active Directory Connector in SSL Mode
- Synchronizing Passwords
- Customizing ACLs
- Customizing the LDAP Schema

Creating and Customizing a Synchronization Profile

A deployment may require you to create new profiles instead of using the default profiles. It may also require you to modify the configurations in these profiles. There are three tools available for creating new profiles. These are:

- The Directory Integration and Provisioning Assistant, a command-line tool for creating profiles and setting various configuration parameters (attributes) in a profile.
- The script `adprofilecfg.sh` that creates the default profiles and sets the minimal information required for the Microsoft Active Directory environment into all the default profiles. This minimal information includes, for example, the Microsoft Active Directory host and port information.

- Oracle Directory Manager, a standalone Java-based GUI tool that enables you to create, modify, and delete profiles. This is suitable when a deployment requires extensive customization.

  See Also:

  - *Oracle Internet Directory Administrator's Guide*, Appendix A, "Syntax for LDIF and Command-Line Tools"
  - "About the adprofilecfg.sh Tool" on page 2-18
  - *Oracle Internet Directory Administrator's Guide*, Chapter 4, "Directory Administration Tools"

Customizing Mapping Rules

You must customize mapping rules when you need to:

- Change domain-level mappings. The domain-level mappings establish how the DIT from Microsoft Active Directory maps to that of Oracle Internet Directory.
- Change what attributes needs to be synchronized.
- Change what transformations (mapping rules) are required to be performed while synchronizing them from the source directory to the target directory.

Domain-Level Mapping

An example of domain level mapping is:

```
DomainRules
%USERBASE%:%USERBASE%:
```

`USERBASE` refers to the container from which the Microsoft Active Directory users and groups must be mapped. Usually, this is the `users` container under the root of the Microsoft Active Directory domain.

For example, if the Microsoft Active Directory host is in the domain `us.mycompany.com`, then the root of the Microsoft Active Directory domain is `us.mycompany.com` and a `user` container under the domain would have a DN value `cn=users, dc=us,dc=mycompany,dc=com`.

For one-to-one domain mapping between Microsoft Active Directory and Oracle Internet Directory, Oracle Internet Directory must be installed with a default realm value of `dc=us,dc=mycompany,dc=com` that would automatically contain a users container under the default realm with a DN value `cn=users,dc=us,dc=mycompany,dc=com`. This enables one-to-one domain mapping between Microsoft Active Directory and Oracle Internet Directory.

If you plan to synchronize only the users under `us.mycmpany.com`, then the domain mapping rule is:

```
DomainRules
cn=users, dc=us, dc=mycompany, dc=com :cn=users, dc=us, dc=mycompany, dc=com
```

This rule enables only the `users` container to be synchronized. Any changes to other entries outside `users` container are not synchronized.

If you later want to synchronize other objects in the domain, the rule can change to

```
DomainRules
dc=us, dc=mycompany, dc=com :dc=us, dc=mycompany, dc=com
```

This rule enables every entry under dc=us,dc=mycompany,dc=com to be synchronized.

Attribute-Level Mapping

An example of attribute-level mapping is:

```
SAMAccountName:1: :user:orclADSAMAccountName: :orclADUser
userPrincipalName: : :user:orclADUserPrincipalName:
:orclADUser:name|userPrincipalName
```

Here, SAMAccountName and userPrincipalName from Microsoft Active Directory are mapped to orclADSAMAccountName and orclADUserPrincipalName respectively.

Adding another attribute to be synchronized requires adding another rule as indicated above. Similarly, if an attribute is no longer to be synchronized, then the corresponding rule simply needs to be removed or commented out.

How to Customize the Mapping Rules

Customizing the mapping rules requires:

- Editing the mapping rules file stored under "" to make necessary modifications as discussed above.
- Once the changes are complete, running the following command:

  ```
  dipassistant mp -profile profile_name -host oid_host -port oid_port -dn DN
  -passwd password odip.profile.mapfile=path_name
  ```

  For example:

  ```
  dipassistant mp -profile ActiveChgImp -host iasdemo.us.oracle.com -port 3060
  -dn cn=orcladmin -passwd welcome1 odip.profile.mapfile= activechgimp.map
  ```

A sample map file is located in the directory $ORACLE_HOME/ldap/odi/conf with the extension of map.master for the various profiles.

Customizing the Search Filter to Get Information from Microsoft Active Directory

By default, the Active Directory connector pulls changes in all the types of objects from the container configured for synchronization. However, if a deployment is interested only in a certain types of changes—for example, only users and groups—then this can be easily achieved by configuring a search filter. The filter is used by the Active Directory connector to filter changes that are not required when it polls the Active Directory for changes. There is an attribute, named searchfilter, in the synchronization profile which stores the filter.

For example, if you are synchronizing changes to users and groups but not Computers objects, then the value of the searchfilter attribute should be: searchfilter=(|(objectclass=group)(&(objectclass=user)(!(objectclass=computer))).

You can use Oracle Directory Manager or the Directory Directory Integration and Provisioning Assistant to update this attribute.

Running the Active Directory Connector in SSL Mode

The Active Directory connector enables secure synchronization between Oracle Internet Directory and Microsoft Active Directory by using SSL between the two

servers. Whether to synchronize in the SSL mode depends on the deployment requirements. For example, synchronizing public data does not require SSL. However, synchronizing sensitive information such as passwords requires SSL. The security settings (hard settings) enable you to synchronize password changes from Oracle Internet Directory to Microsoft Active Directory only in SSL mode with server-only Authentication-that is, SSL Mode 2.

Securing the channel requires:

- SSL between Oracle Internet Directory and the Oracle directory integration and provisioning server
- SSL between Oracle directory integration and provisioning server and Microsoft Active Directory

Although you can enable SSL between Oracle Internet Directory and the Oracle directory integration and provisioning server, or between the Oracle directory integration and provisioning server and Oracle Internet Directory, Oracle Corporation recommends that you completely secure the channel before synchronizing sensitive information. In some cases, such as password synchronization, the synchronization can happen only over SSL.

Configuring SSL requires the following:

- Running the Oracle directory server in the SSL mode as described in *Oracle Internet Directory Administrator's Guide*, Chapter 13, "Secure Sockets Layer (SSL) and the Directory"
- Running the Oracle directory integration and provisioning server in the SSL mode as described in *Oracle Internet Directory Administrator's Guide* Chapter 36, "Security in the Oracle Directory Integration and Provisioning Platform". The SSL mode should be same under which Oracle Internet Directory server was started. The `sslauth` parameter to be specified when starting the Oracle directory integration and provisioning server will be 1 or 2 depending on whether the SSL communication is based on no authentication or server-only authentication.
- Running the Microsoft Active Directory server in the SSL mode. Communication with Microsoft Active Directory over SSL requires SSL Mode 2—that is, server-only authentication. This requires Oracle Internet Directory as well as Directory Integration & Provisioning Server also be run in SSL mode 2.
- Certificates for both Oracle Internet Directory and Microsoft Active Directory and a wallet to store them. See *Oracle Internet Directory Administrator's Guide*, Chapter 13, "Secure Sockets Layer (SSL) and the Directory" for more details.

Note: Oracle Application Server 10*g* does not support SSL in the client-server authentication mode

---

Synchronizing Passwords

You can synchronize passwords from Oracle Internet Directory to Microsoft Active Directory or the reverse.

Synchronizing Passwords from Oracle Internet Directory to Microsoft Active Directory

Before the Active Directory connector can synchronize passwords in this direction, the following are required:

- Adding a mapping rule in the mapping file that enables password synchronization. For example, the mapping rule could be:

  ```
  Userpassword: : :person:unicodepwd: :user
  ```

- Enabling the password policy and the reversible password encryption in the Oracle directory server. This, in turn, requires setting to a value of 1the `orclPwdPolicyEnable` and `orclpwdEncryptionEnable` attributes in the entry `cn=PwdPolicyEntry,cn=common,cn=products,DN of realm`. This can be done either from Oracle Directory Manager or by the `ldapmodify` command.
- Starting these servers in the SSL Mode 2 (server authentication):
  - Oracle directory server
  - Oracle directory integration and provisioning server
  - Microsoft Active Directory server

Synchronizing Passwords from Microsoft Active Directory to Oracle Internet Directory

Synchronizing passwords from Microsoft Active Directory to Oracle Internet Directory is not possible in the Oracle Application Server 10*g* release because passwords in Microsoft Active Directory are not accessible by LDAP clients. However, if a deployment requires passwords to be available in Oracle Internet Directory, then the following two methods are recommended:

- Build a custom plug-in for Microsoft Active Directory that captures a password change and synchronizes it with Oracle Internet Directory
- Manage Active Directory passwords from the Oracle environment. This enables passwords to be available in both Oracle Internet Directory and Microsoft Active Directory because the Active Directory connector can synchronize passwords from Oracle Internet Directory to Microsoft Active Directory.

Customizing ACLs

The default ACLs enable creating, modifying, and deleting users and groups only. Further, they enable users and groups to be created only in the `users` and `groups` containers under the default realm.

Customizing the access control lists (ACLs) is required if:

- You need to synchronize objects other than users and groups
- The containers under which users and groups are synchronized are different from the designated containers. This can be the case when either the preferred containers are not users and groups containers, or they are not under the default realm.

> **See Also:** *Oracle Internet Directory Administrator's Guide*, Chapter 14, "Directory Access Control" for instructions on customizing ACLs

Customizing the LDAP Schema

Customizing the LDAP schema is required if:

- A directory deployment contains schema extensions such as custom object classes and attributes

- The custom attributes must be synchronized from one directory server to the other

Customizing the LDAP schema requires:

- Identifying the schema extensions on the source directory
- Creating those extensions on the target directory before starting the data migration and the synchronization.

> **Note:** Besides creating schema extensions, the attribute which will be required for synchronization also needs to be added into the mapping rules.

Migrating Data Between Directories

Once the Active Directory connector and Plug-in configurations are complete, do the following:

1. Identify the data you want to migrate. You can choose to migrate the entire data in the directory or only a subset.
2. Make sure that the synchronization is not enabled yet.
3. Migrate data from one directory to another by using the Directory Integration and Provisioning Assistant with the `bootstrap` option. Bootstrapping is described in *Oracle Internet Directory Administrator's Guide*, Chapter 37, "Bootstrapping of a Directory in the Oracle Directory Integration and Provisioning Platform".

   Once bootstrapping is accomplished, the profile status attributes are appropriately updated in the synchronization profile by the Directory Integration and Provisioning Assistant.
4. If you have used LDIF file-based bootstrapping, then you need to initialize the `lastchangenumber` value. This can be done by using the Directory Integration and Provisioning Assistant as follows:

   ```
   Dipassistant mp -updlcn
   ```

   This `lastchangenumber` attribute should be set to the value of the last change number in the source directory before you started the bootstrap.
5. If two-way synchronization is required, then enable the export profile and make sure that the change logging option is enabled for the Oracle directory server. Change logging is controlled by the `-l` option while starting Oracle Internet Directory. By default it is set to `TRUE`, meaning that change logging is enabled. If it is set to `FALSE`, then shut down the Oracle directory server and start with the change log enabled by using the Oracle Internet Directory Control Utility.

Managing Integration with Microsoft Windows

This section contains these topics:

- Typical Management Tasks
- Managing the Active Directory External Authentication Plug-in

Typical Management Tasks

Typical ongoing management tasks include:

- Managing synchronization profiles and mapping rules. This includes:
  - Creating new profiles
  - Changing configurations (attributes) in the profile
  - Disabling profiles to allow maintenance and then re-enabling them. Disabling profiles stops synchronization related to that profile.
- Managing mapping rules. This includes:
  - Creating new rules when additional attributes needs to be synchronized
  - Changing existing rules when the way attributes are synchronized needs to change
  - Deleting or commenting out rules not required when a particular attribute is not required to be synchronized
- Managing Access Controls
- Starting and stopping the Oracle directory server and the Oracle directory integration and provisioning server

See Also:

- "Customizing the Active Directory Connector" on page 2-32 for instructions on managing profiles, mapping rules, and access controls
- *Oracle Internet Directory Administrator's Guide*, Appendix A, "Syntax for LDIF and Command-Line Tools" for instructions on starting and stopping servers

Managing the Active Directory External Authentication Plug-in

This section explains how to delete, disable, and re-enable the Active Directory external authentication plug-in.

Deleting the Active Directory External Authentication Plug-in

To delete the Active Directory external authentication plug-in, use these commands.

```
ldapdelete -h host -p port -D cn=orcladmin -w password
"cn=adwhencompare,cn=plugin,cn=subconfigsubentry"

ldapdelete -h host -p port -D cn=orcladmin -w password
"cn=adwhenbind,cn=plugin,cn=subconfigsubentry"
```

Disabling the Active Directory External Authentication Plug-ins

To disable the Microsoft Active Directory external authentication plug-ins, use these two commands:

```
ldapmodify -h host -p port -D cn=orcladmin -w password <<EOF
dn: cn=adwhencompare,cn=plugin,cn=subconfigsubentry
changetype: modify
replace: orclpluginenable
orclpluginenable: 0
EOF

ldapmodify -h host -p port -D cn=orcladmin -w password <<EOF
dn: cn=adwhenbind,cn=plugin,cn=subconfigsubentry
changetype: modify
```

```
replace: orclpluginenable
orclpluginenable: 0
EOF
```

Re-enabling the Active Directory External Authentication Plug-ins

To re-enable the Active Directory external authentication plug-ins, use these two commands:

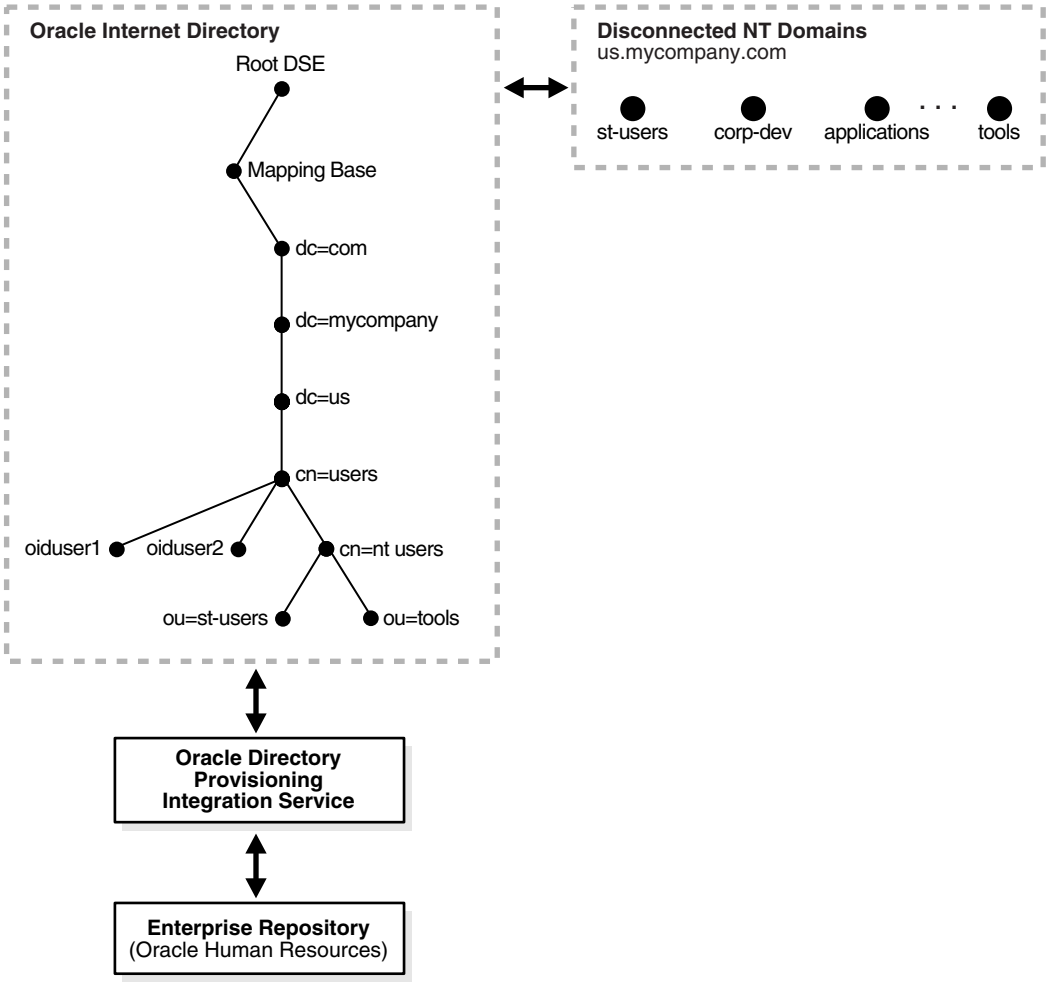
```
ldapmodify -h host -p port -D cn=orcladmin -w password <<EOF
dn: cn=adwhencompare,cn=plugin,cn=subconfigsubentry
changetype: modify
replace: orclpluginenable
orclpluginenable: 1
EOF

ldapmodify -h host -p port -D cn=orcladmin -w password <<EOF
dn: cn=adwhenbind,cn=plugin,cn=subconfigsubentry
changetype: modify
replace: orclpluginenable
orclpluginenable: 1
EOF
```

See Also: "Configuring The Active Directory External Authentication Plug-in" on page 2-30

Integration with Microsoft Windows NT 4.0

Microsoft Windows NT domain users can also be integrated into the environment. Microsoft Windows NT groups are not synchronized to Oracle Internet Directory, nor is information about the members of that group. In this case, each of the Microsoft Windows NT domains can be mapped to a domain object or an organization unit object in Oracle Internet Directory. Typical mapping of Microsoft Windows NT domains to domain containers in the Oracle Internet Directory directory information tree is shown in Figure 2–4.

Figure 2–4 Integration of Oracle Internet Directory DIT with Microsoft Windows NT Domains



Microsoft Windows NT domains are integrated with Oracle Internet Directory so that a minimal user footprint is automatically created in Oracle Internet Directory.

If a user entry exists in Microsoft Windows NT but not in Oracle Internet Directory, then, when that user tries to log in to use the Oracle Application Server components, the auto-registration plug-in creates a shadow entry with minimal footprint information in Oracle Internet Directory. This entry remains in Oracle Internet Directory for the next time the same user tries to log in.

External authentication, with Microsoft Windows NT acting as the external repository, is supported by the use of plug-ins. Ongoing synchronization with the Microsoft Windows NT environment is not supported.

Installing and Configuring Windows NT External Authentication and Auto-Provisioning Plug-ins

The SQL script `oidspnti.sql` installs the plug-ins that enable Oracle Internet Directory for external authentication against the Microsoft Windows primary domain controller and auto provisioning.

To install the script:

1. Verify that the Oracle Internet Directory server is running.

2. Run the script by entering the following command:

```
cd $ORACLE_HOME/ldap/admin
sh oidpnti.sh
```

3. Enter the Oracle Internet Directory host name and port number. The default port number is 389.
4. Enter the password of the Oracle administrator (`orcladmin`), the directory super user.
5. Enter the distinguished name of the container to which the plug-in needs to be applied. Every entry in this container is then authenticated against the Microsoft Windows NT domain. Note that this need not necessarily be the user search base supplied in the Oracle Internet Directory Self-Service Console. All the users under this search base are authenticated externally to the Microsoft Windows NT domain. If more than one value is specified, then use semi-colons (`;`) to separate them.
6. Enter the plug-in request group DN. For security reasons, the plug-in can be invoked only by users belonging to this group. For example, suppose that the Oracle Application Server Single Sign-On administrators are in the group `cn=OracleUserSecurityAdmins,cn=Groups,cn=OracleContext`. If you enter this value for the plug-in request group DN, then only the requests coming from Oracle Application Server Single Sign-On administrators can trigger the external authentication plug-in. You can enter multiple DN values. Use a semicolon (`;`) to separate them. This value is not required, but, for security purposes, should be specified.
7. Choose Auto Registration. The default is `Yes`. Upon registration, each entry is assigned the object class `orclNTUser`.

At the completion of these steps, the plug-in is installed and enabled.

Enabling the Windows NT External Authentication Plug-in

To enable external authentication, enter these two commands:

```
ldapmodify -h host -p port -D cn=orcladmin -w password <<EOF
dn: cn=ntwhencompare,cn=plugin,cn=subconfigsubentry
changetype: modify
replace: orclpluginenable
orclpluginenable: 1
EOF

ldapmodify -h host -p port -D cn=orcladmin -w password <<EOF
dn: cn=ntwhenbind,cn=plugin,cn=subconfigsubentry
changetype: modify
replace: orclpluginenable
orclpluginenable: 1
EOF
```

Disabling the Windows NT External Authentication Plug-in

To disable the external authentication plug-ins, set the value of the attribute `orclpluginenable` to 0 in each of the preceding command.

Enabling Auto Provisioning

To enable auto provisioning, enter the following command:

```
ldapmodify -h host -p port -D cn=orcladmin -w password <<EOF
dn: cn=ntpostsearch,cn=plugin,cn=subconfigsubentry
```

```
changetype: modify
replace: orclpluginenable
orclpluginenable: 1
EOF
```

Disabling Auto Provisioning

To disable auto provisioning, set the value of the attribute orclpluginenable to 0 in the preceding command.

Removing Active Directory External Authentication and Auto Provisioning Plug-ins

To remove external authentication and auto-registration, delete the two plug-in entries from Oracle Internet Directory:

```
ldapdelete -h host -p port D cn=orcladmin -w password
"cn=ntwhencompare,cn=plugin,cn=subconfigsubentry"

ldapdelete -h host -p port -D cn=orcladmin -w password
"cn=ntwhenbind,cn=plugin,cn=subconfigsubentry"

ldapdelete -h host -p port -D cn=orcladmin -w password
"cn=ntpostsearch,cn=plugin,cn=subconfigsubentry"
```

Active Directory External Authentication Plug-in Debugging

If you are experiencing unknown errors, then you can enable the plug-in debugging. To do this:

```
sqlplus ods/odspassword @$ORACLE_HOME/ldap/admin/oidspdon.pls
```

To check the plug-in debugging log:

```
sqlplus ods/ods
select * from plg_debug_log order by id;
```

To delete the plug-in debugging log:

```
sqlplus ods/ods
truncate table plg_debug_log
```

To disable the plug-in debugging:

```
sqlplus ods/ods @$ORACLE_HOME/ldap/admin/oidspdof.pls
```

> **Note:** If you need to change the Active directory external authentication plug-in setup—that is, the information you entered in the installation steps—then rerun the installation script. Before you rerun the script, remove the Active directory external authentication plug-ins by following the preceding instructions.

Troubleshooting Integration with Microsoft Windows

This section contains these topics:

- Troubleshooting Synchronization with Active Directory Connector
- Microsoft Active Directory External Authentication Plug-in

Troubleshooting Synchronization with Active Directory Connector

You can debug the Active Directory connector by using the oditest utility.

To troubleshoot the Active Directory connector

- Run `oditest` specifying `AgentName` as `ProfileName`
- Look at the files `ProfileName.trc` and `ProfileName.aud`

If more than one profiles are enabled, then the tool can be run against each of them.

> **See Also:** *Oracle Internet Directory Administrator's Guide*, Chapter 33, "Oracle Directory Synchronization Service" for instructions on using the `oditest` utility

Debugging the Microsoft Active Directory External Authentication Plug-in

If you are experiencing unknown errors, then you can enable the plug-in debugging. To do this, enter:

```
sqlplus ods/odspassword @$ORACLE_HOME/ldap/admin/oidspdon.pls
```

To check the plug-in debugging log, enter:

```
sqlplus ods/ods
select * from plg_debug_log order by id;
```

To delete the plug-in debugging log:

```
sqlplus ods/ods
truncate table plg_debug_log
```

To disable the plug-in debugging:

```
sqlplus ods/ods @$ORACLE_HOME/ldap/admin/oidspdof.pls
```

Sample LDIF Files Required for Integration with Microsoft Windows

This section contains these sample LDIF files:

- grantrole.ldif
- multidomaindit.ldif
- renameprofile.ldif

grantrole.ldif

```
# This ACL policy grants access to privilaged users to create groups under the
container
# cn=users,dc=us,dc=mycompany,dc=com which is the container for creating users
dn: cn=Users,dc=us,dc=mycompany,dc=com
changetype: modify
add: orclaci
orclaci: access to entry by group="cn=IASAdmins,
cn=groups,cn=OracleContext,dc=us,dc=mycompany,dc=com" added_object_
constraint=(objectclass=orclcontainer) (browse,add)
orclaci: access to entry by group="cn=oracledascreategroup,
cn=groups,cn=OracleContext,dc=us,dc=mycompany,dc=com" added_object_
constraint=(objectclass=orclgroup*) (browse,add) by group="cn=Common Group
Attributes, cn=Groups,cn=OracleContext,dc=us,dc=mycompany,dc=com" (browse)
orclaci: access to entry filter=(&(objectclass=orclgroup)(orclisvisible=false)) by
```

```
groupattr=(owner) (browse, add, delete) by dnattr=(owner) (browse, add, delete) by
group="cn=Common Group Attributes,
cn=Groups,cn=OracleContext,dc=us,dc=mycompany,dc=com" (browse) by * (none)
orclaci: access to entry filter=(&(objectclass=orclgroup)(!(orclisvisible=false)))
by group="cn=oracledascreategroup,
cn=groups,cn=OracleContext,dc=us,dc=mycompany,dc=com" added_object_
constraint=(objectclass=orclgroup) (browse,add) by group="cn=oracledasdeletegroup,
cn=groups,cn=OracleContext,dc=us,dc=mycompany,dc=com" (browse,delete) by
group="cn=oracledaseditgroup,
cn=Groups,cn=OracleContext,dc=us,dc=mycompany,dc=com" (browse) by
groupattr=(owner) (browse, add, delete) by dnattr=(owner) (browse, add, delete) by
group="cn=Common Group Attributes,
cn=Groups,cn=OracleContext,dc=us,dc=mycompany,dc=com" (browse)
orclaci: access to attr=(*) filter=(&(objectclass=orclgroup)(orclisvisible=false))
by groupattr=(owner) (read,search,write,compare) by dnattr=(owner)
(read,search,write,compare) by * (none) by group="cn=Common Group Attributes,
cn=Groups,cn=OracleContext,dc=us,dc=mycompany,dc=com" (read, search, compare)
orclaci: access to attr=(*)
filter=(&(objectclass=orclgroup)(!(orclisvisible=false))) by groupattr=(owner)
(read,search,write,compare) by dnattr=(owner) (read,search,write,compare) by
group="cn=oracledaseditgroup,
cn=groups,cn=OracleContext,dc=us,dc=mycompany,dc=com" (read,search,write,compare)
by group="cn=Common Group Attributes,
cn=Groups,cn=OracleContext,dc=us,dc=mycompany,dc=com" (read, search, compare)

dn: cn=Users,dc=us,dc=mycompany,dc=com
changetype: modify
add: orclentrylevelaci
orclentrylevelaci: access to entry by group="cn=oracledascreategroup,
cn=groups,cn=OracleContext,dc=us,dc=mycompany,dc=com" added_object_
constraint=(objectclass=orclgroup) (browse, add) by group="cn=IASAdmins,
cn=groups,cn=OracleContext,dc=us,dc=mycompany,dc=com" added_object_
constraint=(objectclass=orclcontainer) (browse,add) by * (browse)
```

multidomaindit.ldif

```
#Add the users container
_dn: dc=a,dc=us,dc=mycompany,dc=com
_changetype: add
_dc: a
_objectclass: domain
_
_dn: cn=users,dc=a,dc=us,dc=mycompany,dc=com
_changetype: add
_cn: users
_objectclass: orclcontainer

dn: dc=b,dc=us,dc=mycompany,dc=com
changetype: add
dc: b
objectclass: domain

dn: cn=users,dc=b,dc=us,dc=mycompany,dc=com
changetype: add
cn: users
objectclass: orclcontainer

# ACLS for Users
#Add the acls to create/delete/modify user entries in the users container
dn: cn=users,dc=a,dc=us,dc=mycompany,dc=com
```

```
changetype: modify
add: orclaci

#ACL to add user objects
orclaci: access to entry by group =
"cn=oracledascreateuser,cn=groups,cn=OracleContext,dc=us,dc=mycompany,dc=com"
added_object_constraint=(objectclass=orcluser*) (browse,add)
#ACL to delete user objects
orclaci: access to entry by group="cn=oracledasdeleteuser,
cn=groups,cn=OracleContext,dc=us,dc=mycompany,dc=com" added_object_
constraint=(objectclass=orcluser*) (browse,delete)
#ACL to modify user objects
orclaci: access to attr = (*) by group="cn=orcldasedituser,
cn=Groups,cn=OracleContext,dc=us,dc=mycompany,dc=com" (read, write, search,
compare) by self (read,search,write,compare) by * (noread, nowrite, nocompare)

#Add the acls to create/delete/modify user entries in the users container
dn: cn=users,dc=b,dc=us,dc=mycompany,dc=com
changetype: modify
add: orclaci
#ACL to add user objects
orclaci: access to entry by group =
"cn=oracledascreateuser,cn=groups,cn=OracleContext,dc=us,dc=mycompany,dc=com"
added_object_constraint=(objectclass=orcluser*) (browse,add)
#ACL to delete user objects
orclaci: access to entry by group="cn=oracledasdeleteuser,
cn=groups,cn=OracleContext,dc=us,dc=mycompany,dc=com" added_object_
constraint=(objectclass=orcluser*) (browse,delete)
#ACL to modify user objects
orclaci: access to attr = (*) by group="cn=orcldasedituser,
cn=Groups,cn=OracleContext,dc=us,dc=mycompany,dc=com" (read, write, search,
compare) by self (read,search,write,compare) by * (noread, nowrite, nocompare)

#Change the usersearchbase to point to dc=us,dc=mycompany,dc=com
dn: cn=common, cn=products,cn=oraclecontext,dc=us,d=mycompany,dc=com
changetype: modify
replace: orclCommonUserSearchBase
orclCommonUserSearchBase: dc=us,dc=mycompany,dc=com

#ACLS for Groups
#Add the acls to create/delete/modify group entries in the users container
dn: cn=users,dc=a,dc=us,dc=mycompany,dc=com
changetype: modify
add: orclaci
#ACL to add group objects
orclaci: access to entry by group =
"cn=oracledascreategroup,cn=groups,cn=OracleContext,dc=us,dc=mycompany,dc=com"
added_object_constraint=(objectclass=orclgroup*) (browse,add)
#ACL to delete group objects
orclaci: access to entry by group="cn=oracledasdeletegroup,
cn=groups,cn=OracleContext,dc=us,dc=mycompany,dc=com" added_object_
constraint=(objectclass=orclgroup*) (browse,delete)
#ACL to modify group objects
orclaci: access to attr = (*) by group="cn=orcldaseditgroup,
cn=Groups,cn=OracleContext,dc=us,dc=mycompany,dc=com" (read, write, search,
compare) by self (read,search,write,compare) by * (noread, nowrite, nocompare)

#Add the acls to create/delete/modify group entries in the users container
dn: cn=users,dc=b,dc=us,dc=mycompany,dc=com
changetype: modify
```

```
add: orclaci
#ACL to add group objects
orclaci: access to entry by group =
"cn=oracledascreategroup,cn=groups,cn=OracleContext,dc=us,dc=mycompany,dc=com"
added_object_constraint=(objectclass=orclgroup*) (browse,add)
#ACL to delete group objects
orclaci: access to entry by group="cn=oracledasdeletegroup,
cn=groups,cn=OracleContext,dc=us,dc=mycompany,dc=com" added_object_
constraint=(objectclass=orclgroup*) (browse,delete)
#ACL to modify group objects
orclaci: access to attr = (*) by group="cn=orcldaseditgroup,
cn=Groups,cn=OracleContext,dc=us,dc=mycompany,dc=com" (read, write, search,
compare) by self (read,search,write,compare) by * (noread, nowrite, nocompare

#Change the GroupSearchBase to point to dc=us,dc=mycompany,dc=com
dn: cn=common, cn=products,cn=oraclecontext,dc=us,d=mycompany,dc=com
changetype: modify
replace: orclCommonGroupSearchBase
orclCommonGroupSearchBase: dc=us,dc=mycompany,dc=com
```

renameprofile.ldif

```
#Modify the name of the profile
dn: orclodipagentname=activechgimp,cn=subscriber profile,cn=changelog
subscriber,cn=oracle internet directory
changetype: modrdn
newrdn: activechgimp1
deleteoldrdn: 1

#Remove the privileges given to the old profile and add the privileges to the new
profile
dn: cn=odipgroup,cn=odi,cn=oracle internet directory
changetype: modify
delete: uniquemember
uniquemember: orclodipagentname=activechgimp,cn=subscriber profile,cn=changelog
subscriber,cn=oracle internet directory
-
add: uniquemember
uniquemember: orclodipagentname=activechgimp1,cn=subscriber profile,cn=changelog
subscriber,cn=oracle internet directory
You must include an introductory element, such as a Para, before inserting the
first Sect1 element. This requirement prevents arriving at an empty XHTML page for
the chapter if you have selected the option of breaking at Sect1 when generating
XHTML output
```

3

Windows Native Authentication

To complete the integration of Microsoft Active Directory with Oracle Collaboration Suite, you must deploy OracleAS Single Sign-On for automatic sign-on, also known as Windows native authentication. The terms automatic sign-on and Windows native authentication are synonymous. For the remainder of the document, the latter term is used.

The following topics guide you through the process of deploying Windows native authentication from a Windows desktop:

Overview of Windows Native Authentication

Windows native authentication is an authentication scheme for those who use Internet Explorer on Windows 2000. When this feature is enabled in OracleAS Single Sign-On, users log in to single sign-on partner applications automatically using Kerberos credentials obtained when the user logs in to a Windows 2000 computer.

Using the SPNEGO protocol, browsers that are Internet Explorer 5.0 and greater can automatically pass the user's Kerberos credentials to a Kerberos-enabled Web server when the server request these credentials. The Web server can then decrypt the credentials and authenticate the user.

Although SPNEGO supports both Kerberos version 5 and NTLM authentication schemes, OracleAS release 9.0.4 supports only Kerberos version 5 with SPNEGO.

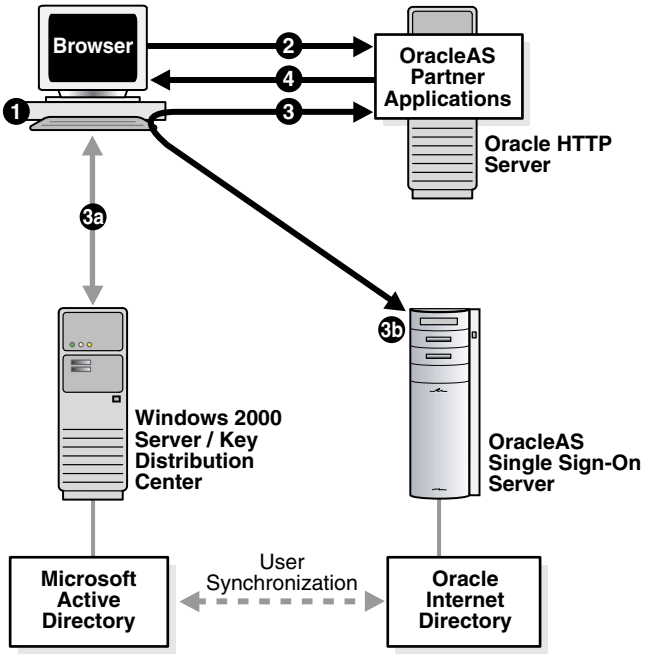
Note: Although this document refers only to Windows 2000, Windows native authentication is also supported on the Windows XP platform.

How Windows Native Authentication Works

The following steps, illustrated in Figure 3–1 on page 3-2, describe what happens when a user tries to access a single-sign-on-protected application:

1. The user logs in to a Kerberos realm, or domain, on a Windows 2000 computer.
2. The user attempts to access a single-sign-on partner application using Internet Explorer.
3. The application redirects the user to the single sign-on server for authentication. As part of this redirection, the following occurs:
   a. The browser obtains a Kerberos session ticket from the Key Distribution Center (KDC).
   b. The single sign-on server verifies the Kerberos session ticket and returns the user to the requested URL.
4. The application provides content to the user.

Figure 3–1 Flow for Windows Native Authentication



The user logs out of this application and single sign-on applications accessed subsequently by logging out of the Windows computer.

System Requirements

Windows native authentication is intended for intranet Web applications. Your intranet deployment must have the following:

- Windows 2000 server with Microsoft Active Directory
- Kerberos service account established for single sign-on server
- OracleAS release 9.0.4 infrastructure installed

> **Note:** The configurations that follow assume that the OracleAS infrastructure is installed on UNIX, but it can be installed on Windows instead.

- Single sign-on middle tier configured to use a Kerberos realm
- Synchronization between Microsoft Active Directory and Oracle Internet Directory
- Oracle Internet Directory configured to use the Windows authentication plugin

Configuring Windows Native Authentication

Setting up Windows native authentication requires that Oracle Internet Directory, the single sign-on server, and the user's browser all be configured.

Perform these configuration tasks in the order listed:

- Verify That Microsoft Active Directory Is Set Up and Working
- Install Oracle Internet Directory and OracleAS Single Sign-On
- Synchronize Oracle Internet Directory with Microsoft Active Directory
- Configure Oracle Internet Directory to Use Windows Authentication Plugin
- Verify That Synchronization and the Authentication Plugin Are Working
- Configure the Single Sign-On Server
- Configure the End User Browser
- Reconfigure Local Accounts

Verify That Microsoft Active Directory Is Set Up and Working

Consult documentation for the Windows 2000 server to ensure that Microsoft Active Directory is set up and working.

Install Oracle Internet Directory and OracleAS Single Sign-On

Install Oracle Internet Directory and OracleAS Single Sign-On. To determine which deployment configuration suits your installation, see Chapter 9, "Advanced Configurations" in the *Oracle Application Server Single Sign-On Administrator's Guide 10g (9.0.4)*. For installation instructions, see *Oracle Application Server 10g Installation Guide*.

Synchronize Oracle Internet Directory with Microsoft Active Directory

User entries in Oracle Internet Directory must be synchronized with user entries in Microsoft Active Directory. To learn how to synchronize Oracle Internet Directory with Microsoft Active Directory, see the Oracle Internet Directory Administrator's Guide.

Configure Oracle Internet Directory to Use Windows Authentication Plugin

See the Oracle Internet Directory Administrator's Guide.

Verify That Synchronization and the Authentication Plugin Are Working

Verify that you have synchronized user entries between the two directories; then verify that the Windows authentication plugin is working. You perform this step by trying to log in to the single sign-on server:

1. Go to the login page:

   `http://host:port/pls/orasso`

2. Enter your user name in this format:

user_name@active_directory_domain

then enter your password.

Configure the Single Sign-On Server

Complete the following tasks to configure the single sign-on server.

- Set Up a Kerberos Service Account for the Single Sign-On Server
- Configure the Single Sign-On Server to Use the Sun JAAS Login Module
- Configure the Single Sign-On Server as a Secured Application

Set Up a Kerberos Service Account for the Single Sign-On Server

Configure a kerberos realm on the single sign-on middle tier; then create a service account for the single sign-on server in Microsoft Active Directory. Finally, create a keytab file for the single sign-on server, mapping the service principal to the account name.

1. Configure the krb5.conf file/etc/krb5/krb5.conf (*system_drive*:\krb5\krb5 on Windows) on the middle tier. You do this by updating the file to look like the following example:

```
[libdefaults]
default_realm = ADUSERS.ACME.COM
[realms]
ADUSERS.ACME.COM = {
   kdc = kdc.acme.com
   }
[domain_realm]
.acme.com = ADUSERS.ACME.COM
```

   where `ADUSERS.ACME.COM` is the default realm of Microsoft Active Directory, `kdc.acme.com` is the host name of the KDC, and `.acme.com` is the DNS domain name of the UNIX computer. Be sure to replace the example values given with values suitable for your installation. These values appear in boldface in the example. The file is found at /etc/krb5 on UNIX systems and at *system_drive*:\krb5 on Windows systems.

   Note: The realm name in krb5.conf is case sensitive and should match the realm name in Microsoft Active Directory. The realm name is usually uppercase.

2. Synchronize system clocks between the single sign-on middle tier and the Windows 2000 server. If you omit this step, authentication fails because of clock skew errors.

3. Check the port number of the Kerberos server on the single sign-on computer. The port where the Kerberos server listens is picked from /etc/services by default. On Windows systems, the services file is found at *system_drive*:\WINNT\system32\drivers\etc. The service name is Kerberos. Typically the port is set to `88/udp` and `88/tcp` on the Windows 2000 server. When added correctly to the services file, the entries for these port numbers look like this:

```
kerberos5       88/udp          kdc             # Kerberos key server
kerberos5       88/tcp          kdc             # Kerberos key server
```

4. In the hosts file, located in the same directory as the services file, check the entry for the single sign-on middle tier. The fully qualified host name of the single sign-on computer must appear after the IP address and before the short name. Here is an example of a correct entry:

   ```
   130.111.111.111 sso.acme.com sso loghost
   ```

5. Log in to the Active Directory Management tool on the Windows 2000 server; then click **Users -> New -> user**.

   Enter the name of the single sign-on host, omitting the domain name. If, for example, the host name is `sso.acme.com`, you enter only `sso`. This is the account name in Active Directory.

   Note the password that you assigned to the account. You will need it later. Do *not* choose

   User must change password at next logon.

6. Create a keytab file for the single sign-on server, mapping the account name to the service principal name. You perform both tasks by issuing the following command on the Windows 2000 server:

   ```
   C:> Ktpass -princ HTTP/sso.acme.com@ADUSERS.ACME.COM -pass password -mapuser
   sso -out sso.keytab
   ```

   where `-princ` is the service principal. This value must be specified using the format `HTTP/`*`single_sign-on_host_name`*`@`*`KERBEROS_REALM_NAME`*. Note that `HTTP` and the Kerberos realm must be uppercase.

   `-pass` is the account password that you obtained in step 4. `-mapuser` is the account name of the single sign-on middle tier. You created this account in step 4. `-out` is the output file that stores the service key.

   Again, be sure to replace the example values given with values suitable for your installation. These values appear in boldface in the example.

   > **Note:** If ktpass is not found on your computer, download the Windows resource kit to obtain the utility.

7. Copy or FTP the keytab file, sso.keytab, created in step 4, to the single sign-on middle tier, placing it in $ORACLE_HOME/j2ee/OC4J_SECURITY/config.

   Be sure to give the Web server uid on the single sign-on middle tier read permission for the file.

Configure the Single Sign-On Server to Use the Sun JAAS Login Module

1. Modify $ORACLE_HOME/opmn/conf/opmn.xml to include the following four command line parameters for JVM:

   ```
   -Djavax.security.auth.useSubjectCredsOnly=false
   -Doracle.security.jazn.config=$ORACLE_HOME/j2ee/OC4J_SECURITY/config/jazn.xml
   -Djava.security.krb5.realm=default_realm_in_Active_Directory
   -Djava.security.krb5.kdc=Active_Directory_host_name
   ```

   These parameters should be added to the OC4J_SECURITY process configuration section of opmn.xml. Add them as values to both the "start-parameters" and "stop-parameters" category id tags.

2. Modify $ORACLE_HOME/j2ee/OC4J_SECURITY/config/jazn.xml to point to an XML provider.

```
<jazn provider="XML" location="./jazn-data.xml" />
```

Comment the following line if it is not commented already:

```
<jazn provider="LDAP" location="ldap://myoid.us.oracle.com:389" />
```

3. Add the entry that follows to $ORACLE_HOME/j2ee/OC4JSECURITY/config/jazn-data.xml. This step configures the single sign-on server to use Krb5LoginModule, the Sun JAAS login module.

In the XML entry, `KeyTab` designates the location of the keytab file. `principal` is the service principal name for the single sign-on server. For consistency, the example keytab file and principle have been retained in the entry. Be sure to replace the values that appear in boldface with actual values.

You can either cut and paste the entry provided here or copy and paste the sample file, $ORACLE_HOME/sso/conf/wna-jazn-data.xml.

```
<jazn_data>
  <jazn-loginconfig>
  .
  .
  .
    <application>
      <name>com.sun.security.jgss.accept</name>
      <login-modules>
      <login-module>
        <class>com.sun.security.auth.module.Krb5LoginModule</class>
        <control-flag>required</control-flag>
        <options>
          <option>
            <name>debug</name>
            <value>false</value>
          </option>
          <option>
            <name>addAllRoles</name>
            <value>true</value>
          </option>
          <option>
            <name>useKeyTab</name>
            <value>true</value>
          </option>
          <option>
            <name>keyTab</name>
            <value>Oracle_home/j2ee/OC4J_SECURITY/config/sso.keytab</value>
          </option>
          <option>
            <name>principal</name>
            <value>HTTP/sso.acme.com</value>
          </option>
          <option>
            <name>doNotPrompt</name>
            <value>true</value>
          </option>
          <option>
            <name>storeKey</name>
            <value>true</value>
          </option>
```

```
        </options>
      </login-module>
      </login-modules>
    </application>
    .
    .
    .
  </jazn-loginconfig>
</jazn-data>
```

Configure the Single Sign-On Server as a Secured Application

1. Add the entry that follows to $ORACLE_HOME/j2ee/OC4J_SECURITY/applications/sso/web/WEB-INF/web.xml.

   Cut and paste the entry provided here or copy and paste the sample file located at $ORACLE_HOME/sso/conf/wna-web.xml.

```
<web-app>
.
.
.
  <security-role>
    <role-name>{{PUBLIC}}</role-name>
  </security-role>
  <security-constraint>
    <web-resource-collection>
      <web-resource-name>SSO</web-resource-name>
      <url-pattern>auth</url-pattern>
    </web-resource-collection>
    <!-- authorization -->
    <auth-constraint>
      <role-name>{{PUBLIC}}</role-name>
    </auth-constraint>
  </security-constraint>
  <!-- authentication -->
  <login-config>
    <auth-method>BASIC</auth-method>
  </login-config>
  .
  .
  .
</web-app>
```

2. Configure a Kerberos service name for the single sign-on server in $ORACLE_HOME/j2ee/OC4J_SECURITY/application-deployments/sso/orion-application.xml. You do this by adding the entry that follows. Be sure to replace the values that appear in boldface with actual values. You may use the sample file in $ORACLE_HOME/sso/conf instead.

```
<orion-application>
.
.
.
  <security-role-mapping name="{{PUBLIC}}">
    <group name="{{PUBLIC}}" />
  </security-role-mapping>
  <jazn provider="LDAP" location="ldap://directory_server.domain:port"
  default-realm="default_realm_in_Oracle_Internet_Directory">
  <jazn-web-app auth-method="WINDOWS_KERBEROS_AUTH"/>
  <property name="kerberos-servicename" value="HTTP@sso.acme.com"/>
```

```
  </jazn>
  .
  .
  .
</orion-application>
```

> **Note:** If your directory has just one realm, you may omit the `default-realm` parameter. If the directory has more than one realm, enter only the realm name, not the realm DN. If, for example, your realm has a DN of `dc=uk,dc=oracle,dc=com`, the realm name is `uk`.

3. Configure the single sign-on server to use the Kerberos authentication plugin. In $ORACLE_HOME/sso/conf/policy.properties, designate the Kerberos plugin as the default authentication plugin.

   Edit the `MediumSecurity_AuthPlugin` parameter to look like this:

   ```
   MediumSecurity_AuthPlugin = oracle.security.sso.server.auth.SSOKerbeAuth
   ```

4. Restart the single sign-on middle tier. For instructions, see "Stopping and Starting the Single Sign-On Middle Tier" in Chapter 2 of the *Oracle Application Server Single Sign-On Administrator's Guide 10g (9.0.4)*.

Configure the End User Browser

Configure Internet Explorer to use Windows native authentication. Depending upon your browser, configuration is a two-part process:

- Internet Explorer 5.0 and Greater
- Internet Explorer 6.0 Only

Internet Explorer 5.0 and Greater

1. Click the following in succession:
   - Tools
   - Internet Options
   - Security
   - Local intranet
   - Sites
2. In the Local intranet dialog box, choose **Include all sites that bypass the proxy** server; then click **Advanced**.
3. In the advanced version of the Local intranet dialog box, enter the URL of the single sign-on middle tier. Here is an example:

   ```
   http://sso.mydomain.com
   ```

4. Click **OK** to exit the Local intranet dialog boxes.
5. In the Internet Options dialog box, click the **Security** tab; then click **Local** intranet; then **Custom Level**.
6. In the Security Settings dialog box, scroll down to the User Authentication section and then choose **Automatic logon only in Intranet zone**.

7. Click **OK** to exit the Security Settings dialog box.
8. Click the following in succession:
   - Tools
   - Internet Options
   - Connections
9. On the **Connections** tab, click **LAN Settings**.
10. Check that you have the correct address and port number for the proxy server; then click **Advanced**.
11. In the Proxy Settings dialog box, in the **Exceptions** section, make sure that you have entered the domain name for the single sign-on server (acme.com in the example).
12. Click **OK** to exit the Proxy Settings dialog box.

Internet Explorer 6.0 Only

If you are using Internet Explorer 6.0, perform steps 1 through 12 in "Internet Explorer 5.0 and Greater"; then add the following steps:

1. Click the following in succession:
   - Tools
   - Internet Options
   - Advanced
2. On the **Advanced** tab, scroll down to the Security section.
3. Choose **Enable Integrated Windows Authentication (requires restart)**.

Reconfigure Local Accounts

Now that you have successfully configured Windows native authentication, you must reconfigure accounts for orcladmin and other local Windows users. These are users whose accounts are in Oracle Internet Directory. If you omit this task, these users will not be able to log in.

Use the administration console for Oracle Internet Directory to perform these steps:

1. Add the `orclADUser` class to the local user entry in Oracle Internet Directory.
2. Add the login ID of the local user to the `orclSAMAccountName` attribute in the user's entry. For example, the login ID of the orcladmin account is `orcladmin`.
3. Add the local user to the `exceptionEntry` property of the external authentication plugin.

Fallback Authentication

Only browsers that are Internet Explorer 5.0 or greater support SPNEGO-Kerberos authentication. OracleAS Single Sign-On provides fallback authentication support for unsupported browsers such as Netscape Communicator. Depending upon the type of browser and how it is configured, you are presented with the single sign-on login form or the HTTP basic authentication dialog box. In either case, you must provide a user name and password. The user name consists of the Kerberos realm name and the user ID. It must be entered this way:

domain_name\user_id

For example:

```
acme\jdoe
```

Note that the user name and password are case sensitive. Note, too, that password policies for Microsoft Active Directory do not apply.

Fallback authentication is performed against Microsoft Active Directory, using an external authentication plugin for Oracle Internet Directory.

Notes:

- HTTP basic authentication does not support logout. To clear their credentials from the browser cache, users must close all opened browsers. Alternatively, they can log out of the Windows computer.
- In cases where basic authentication is invoked, users must set their language preference manually in Internet Explorer. This is accomplished by navigating to Tools -> Internet Options -> Languages and then adding the desired language.

Login Scenarios

Users may encounter a number of different login behaviors within Internet Explorer depending upon which version they are using. Table 3–1 on page 3-10 shows under what circumstances automatic sign-on and fallback authentication are invoked.

Table 3–1 Single Sign-On Login Options in Windows Internet Explorer

Browser Version	Desktop Platform	Desktop Authentication Type	Integrated Authentication in Internet Explorer Browser	Single Sign-On Login Type
>= 5.0.1	Windows 2000/XP	Kerberos version 5	On	Automatic sign-on
>= 5.0.1 and < 6.0	Windows 2000/XP	Kerberos version 5	Off	Single sign-on
>= 6.0	Windows 2000/XP	Kerberos version 5 or NTLM	Off	HTTP basic authentication
>= 5.0.1 and < 6.0	Windows NT/2000/XP	NTLM	On or off	Single sign-on
>= 6.0	NT/2000/XP	NTLM	On	Single sign-on
>= 5.0.1	Windows 95, ME, Windows NT 4.0	N/A	N/A	Single sign-on
< 5.0.1	N/A	N/A	N/A	Single sign-on
All other browsers	All other platforms	N/A	N/A	Single sign-on

Index

Symbols

Numerics

A

B

C

D

E

F

H

I

J