# Oracle® Identity Management

Guide to Delegated Administration

10*g* (10.1.4.0.1)

**B15996-01**

July 2006

ORACLE®

Oracle Identity Management Guide to Delegated Administration, 10*g* (10.1.4.0.1)

B15996-01



Primary Author: Don Gosselin

# Contents

## A Elements in the Oracle Internet Directory Self-Service Console User Interface

## B Troubleshooting Oracle Delegated Administration Services

## List of Figures

## List of Tables

# Preface

*Oracle Identity Management Guide to Delegated Administration* describes how to perform delegated administration for Oracle Internet Directory.

## Audience

*Oracle Identity Management Guide to Delegated Administration* is intended for anyone who performs delegated administration for Oracle Internet Directory, including the following tasks:

- Installing and configuring of Oracle Delegated Administration Services
- Starting and stopping Oracle Delegated Administration Services
- Creating applications by using Oracle Delegated Administration Services
- Configuring Oracle Delegated Administration Services
- Using the Oracle Internet Directory Self-Service Console

To use this document, you should be familiar with the UNIX operating system and have some familiarity with Lightweight Directory Access Protocol (LDAP). You should also have an understanding of how to administer Oracle Internet Directory. Refer to the *Oracle Internet Directory Administrator's Guide* for more information on Oracle Internet Directory administration.

## Documentation Accessibility

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

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

### Accessibility of Code Examples in Documentation

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

### Accessibility of Links to External Web Sites in Documentation

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

### TTY Access to Oracle Support Services

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

## Related Documents

For more information, see the Oracle Application Server Documentation Library, especially:

- *Oracle Identity Management Infrastructure Administrator's Guide*
- *Oracle Internet Directory Administrator's Guide*
- *Oracle Identity Management Integration Guide*
- *Oracle Identity Management Application Developer's Guide*
- *Oracle Identity Management User Reference*

Printed documentation is available for sale in the Oracle Store at

`http://oraclestore.oracle.com/`

## Conventions

The following text conventions are used in this document:

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

# Part I

# Oracle Delegated Administration Services

This part introduces the concepts, architecture, and components of Oracle Delegated Administration Services, and tells you how to install, configure, and administer Oracle Delegated Administration Services.

Part I contains the following chapters:

# 1

# Getting Started with Oracle Delegated Administration Services

This chapter describes Oracle Delegated Administration Services, a framework consisting of pre-defined, Web-based units for building administrative and self-service consoles. These consoles can be used by delegated administrators and users to perform specified directory operations.

It contains these topics:



> **Note:** Oracle Delegated Administration Services is only used for managing information that is stored in Oracle Internet Directory. To manage information that is stored in third-party or heterogeneous directory environments, consider using Oracle Access Manager, which provides a full range of identity administration and security functions. Oracle Access Manager functionality includes Web single sign-on, user self-service and self-registration, sophisticated workflow functionality, reporting and auditing, policy management, dynamic group management, and delegated administration.

## About Delegated Administration

Delegated administration is an important feature of the Oracle Identity Management infrastructure. It enables you to store all data for users, groups, and services in a central directory, while distributing the administration of that data to various administrators and end users. It does this in a way that respects the various security requirements in your environment.

Suppose, for example, that your enterprise stores all user, group, and services data in a central directory, and requires one administrator for user data, and another for the e-mail service. Or suppose that it requires the administrator of Oracle Financials to fully control user privileges, and the administrator of OracleAS Portal to fully control the Web pages for a specific user or group. Delegated administration as provided by the Oracle Identity Management infrastructure enables all of these administrators with their diverse security requirements to administer the centralized data in a way that is both secure and scalable. The following privileges can be delegated with Oracle Delegated Administration Services:

- Creation, editing, and deletion of users and groups
- Assignment of privileges to users and groups
- Management of services and accounts
- Configuration of Oracle Delegated Administration Services
- Resource management of Oracle Reports and Oracle Application Server Forms Services

> **See Also:** The chapter on delegation of privileges for an Oracle technology deployment in *Oracle Internet Directory Administrator's Guide* for more information about delegated administration

# About Oracle Delegated Administration Services

Oracle Delegated Administration Services is a set of pre-defined, Web-based units for performing directory operations on behalf of a user. It frees directory administrators from the more routine directory management tasks by enabling them to delegate specific functions to other administrators and to end users. It provides most of the functionality that directory-enabled applications require, such as creating a user entry, creating a group entry, searching for entries, and changing user passwords.

You can use Oracle Delegated Administration Services to develop your own tools for administering application data in the directory. Alternatively, you can use the Oracle Internet Directory Self-Service Console, a tool based on Delegated Administration Services. This tool comes ready to use with Oracle Internet Directory.

> **See Also:** Chapter 3, "Working with the Oracle Internet Directory Self-Service Console"

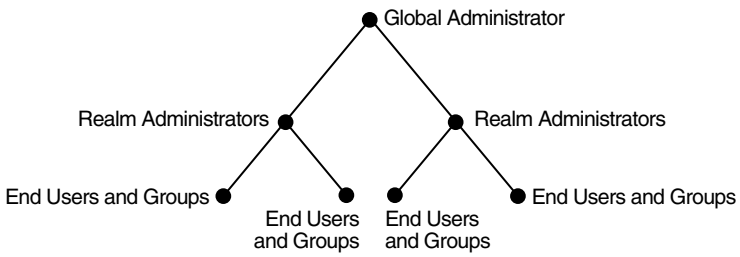
This section contains these topics:

- Delegation of Directory Data Administration
- How Oracle Delegated Administration Services Works
- How Oracle Delegated Administration Services Provides Secure Access to the Directory

## Delegation of Directory Data Administration

Applications built by using Oracle Delegated Administration Services enable you to grant a specific level of directory access to each type of user. For example, look at Figure 1–1, which shows the various administrative levels in a hosted environment.

***Figure 1–1 Administrative Levels in a Hosted Environment***



The global administrator, with full privileges for the entire directory, can delegate to realm administrators the privileges to create and manage the realms for hosted companies. These administrators can, in turn, delegate to end users and groups the privileges to change their application passwords, personal data, and preferences. Each type of user can thus be given the appropriate level of privileges.

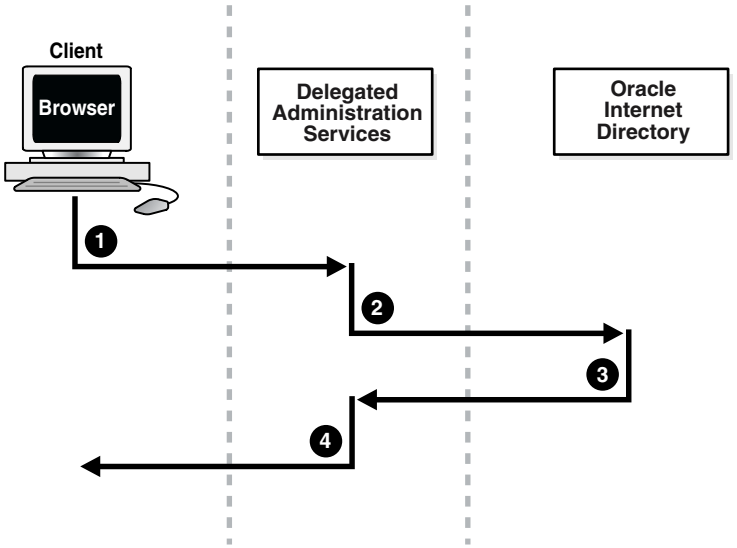
## How Oracle Delegated Administration Services Works

Oracle Delegated Administration Services is a J2EE application that is deployed on an Oracle Containers for J2EE (OC4J) instance. Oracle Delegated Administration Services performs the following basic tasks:

1. Receive requests from clients
2. Process those requests—by either retrieving or updating data in Oracle Internet Directory—and compile the LDAP result into an HTML page
3. Send the HTML page back to the client Web browser

Figure 1–2 shows the flow of information between components in a Oracle Delegated Administration Services environment.

***Figure 1–2 Flow of Information Between Components in a Oracle Delegated Administration Services Environment***




As Figure 1–2 shows:

1. The user, from a browser and using HTTP, sends to Oracle Delegated Administration Services a request containing a directory query.
2. Oracle Delegated Administration Services receives the request and launches the appropriate servlet. This servlet interprets the request, and sends it to Oracle Internet Directory by using LDAP.
3. Oracle Internet Directory sends the LDAP result to the Oracle Delegated Administration Services servlet.
4. The Oracle Delegated Administration Services servlet compiles the LDAP result into an HTML page, and sends it to the client Web browser.

## How Oracle Delegated Administration Services Provides Secure Access to the Directory

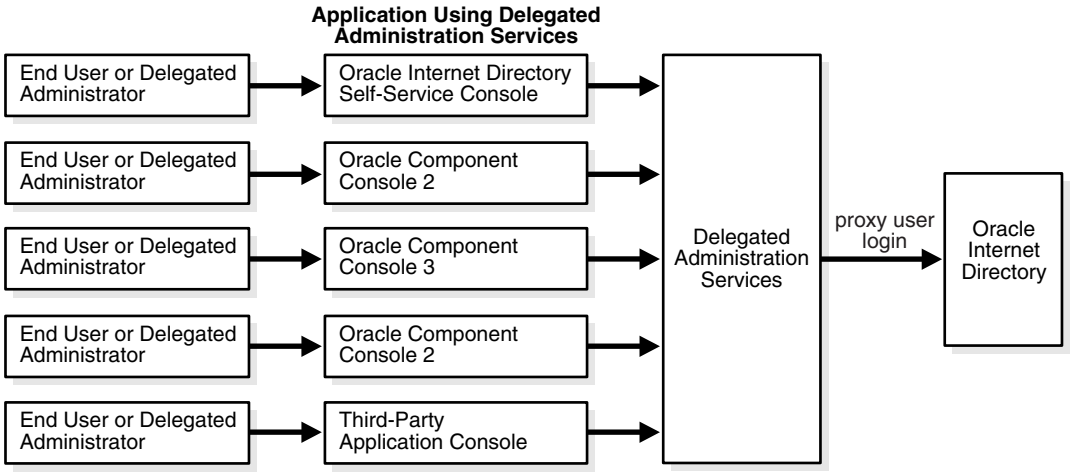
When a user logs into an Oracle component, that component may need to obtain information from the directory on the end user's behalf—for example, the password verifier. To do this, the component typically logs into the directory as a proxy user, a feature that enables it to switch its identity to that of the end user.

A problem, however, is that the greater the number of components logging into the directory as proxy users, the greater the risk of a malicious user accessing the directory as a proxy user. To prevent this security problem, the Oracle Delegated Administration Services centralizes proxy user access.

In a Oracle Delegated Administration Services environment, each component, instead of logging into the directory as a proxy user, logs into the central Oracle Delegated Administration Services. Oracle Delegated Administration Services then logs into the directory as a proxy user, switches its identity to that of the end user, and performs operations on that user's behalf. Centralizing proxy user directory access in this way replaces the less secure strategy of granting proxy user access to every component accessing the directory.

Figure 1–3 shows the proxy user feature in an Oracle Delegated Administration Services environment. End users or delegated administrators log in to a central Oracle Delegated Administration Services. They do this by using the Oracle Internet Directory Self-Service Console, the consoles of other Oracle components such as OracleAS Portal, or those of third-party applications. The Oracle Delegated Administration Services then logs into Oracle Internet Directory as a proxy user.

***Figure 1–3 Centralization of the Proxy User Feature in the Oracle Delegated Administration Services***




# Installing and Configuring Oracle Delegated Administration Services

This section tells you how to install and configure Oracle Delegated Administration Services. It contains these topics:

- Task 1: Install Oracle Delegated Administration Services
- Task 2: Verify that Oracle Delegated Administration Services Is Running
- Task 3: Configure the Default Identity Management Realm
- Task 4: Configure User Entries

- Location of Log Files for Components in the Oracle Delegated Administration Services Environment

  **See Also:** Appendix B, "Troubleshooting Oracle Delegated Administration Services" for information on how to troubleshoot Oracle Delegated Administration Services

## Task 1: Install Oracle Delegated Administration Services

By default, Oracle Delegated Administration Services is installed as part of Oracle Internet Directory 10*g* (10.1.4.0.1). However, during the installation process you can also choose to install Oracle Delegated Administration Services by itself. In this manner, you can install multiple instances of Oracle Delegated Administration Services on separate servers that communicate with a single instance of Oracle Application Server.

---

**Note:** During installation,Oracle Delegated Administration Services is deployed in the OC4J_SECURITY instance. Because most of the Oracle Delegated Administration Services setup depends on this instance, its important that the name of this instance not be changed.

---

**See Also:**

- Oracle Application Server installation documentation for your operating system
- *Oracle Application Server Administrator's Guide* for information on how to use the SSL Configuration Tool, which simplifies and automates post-installation SSL configuration for common Oracle Application Server topologies

## Task 2: Verify that Oracle Delegated Administration Services Is Running

You can use Oracle Enterprise Manager 10*g* Application Server Control Console to verify that Oracle Delegated Administration Services is running as follows:

1. Go to the standalone console for the infrastructure instance of Oracle Enterprise Manager that you want to administer by entering the host name of the computer hosting the Oracle Application Server instance and the port number of Oracle Enterprise Manager. The default port number is `1810`, but it may be configured in increments of one, up to `1816`.
2. Log in using the credentials of an Oracle Application Server administrator.
3. From the **Standalone Instances** section of the Farm page, choose the appropriate Oracle Application Server instance.
4. Locate **OC4J_SECURITY** in the **System Components** table. The Status column will contain one of the following:
   - An up arrow, which indicates the component is up and running
   - A down arrow, which indicates the component is down and not running
   - An icon in the shape of a stopwatch, which indicates that the Application Server Control Console is unable to determine the status of the component

If Oracle Delegated Administration Services is not running, then start it by following the instructions in Starting and Stopping Oracle Delegated Administration Services on page 1-7.

> **See Also:** *Oracle Internet Directory Administrator's Guide* for more information on how to work with the Oracle Enterprise Manager 10*g* Application Server Control Console

Alternatively, you can verify that Oracle Delegated Administration Services are running by using the Identity Management Grid Control Plug-in, as described in the *Oracle Identity Management Infrastructure Administrator's Guide*, or by using the following command-line procedures:

### Step 1: Verify that the Oracle HTTP Server Is Running

To do this, use the following command:

```
$ORACLE_HOME/opmn/bin/opmnctl status
```

> **See Also:** Table 1–1 on page 1-7 to find log file locations for components in the Oracle Delegated Administration Services environment

### Step 2: Verify that the Oracle Application Server Single Sign-On Server Is Running

Using any browser, enter:

```
http://host_name:port_number/orasso/
```

where *host_name* is the name of the computer on which the Oracle HTTP Server is running, and *port_number* is the corresponding port number. The default port number of the Oracle HTTP Server is 7777. Try to log in by using the Oracle Application Server Single Sign-On login window.

### Step 3: Verify that Oracle Delegated Administration Services Is Running

Using any browser, enter:

```
http://host_name:port_number/oiddas/
```

where *host_name* is the name of the computer on which the Oracle HTTP Server is running, and *port_number* is the corresponding port number. The default port number of the Oracle HTTP Server is 7777. This displays the Oracle Delegated Administration Services home page.

If Oracle Delegated Administration Services is not running, then start it by following the instructions in "Starting and Stopping Oracle Delegated Administration Services" on page 1-7.

## Task 3: Configure the Default Identity Management Realm

To do this, follow the instructions in the section "Configuring an Identity Management Realm" on page 5-2.

## Task 4: Configure User Entries

To do this, follow the instructions in the section "Configuring User Entries" on page 5-5.

## Location of Log Files for Components in the Oracle Delegated Administration Services Environment

Table 1–1 tells you where to find the log files for components in the Oracle Delegated Administration Services environment.

***Table 1–1 Log Files for Components In Oracle Delegated Administration Services Environment***

| Application | Log File Location |
|---|---|
| Oracle HTTP Server | $*ORACLE_HOME*/Apache/Apache/logs |
| Oracle Containers for J2EE (OC4J) | $*ORACLE_HOME*/j2ee/OC4J_SECURITY/log |
| Oracle Delegated Administration Services | $*ORACLE_HOME*/opmn/logs/OC4J~OC4J_SECURITY~default_island~1 |
| Oracle Process Manager and Notification Server | $*ORACLE_HOME*/opmn/logs |

# Starting and Stopping Oracle Delegated Administration Services

You can use the command line, the Oracle Enterprise Manager 10*g* Application Server Control Console, or the Identity Management Grid Control Plug-in to start and stop Oracle Delegated Administration Services, as described in the following topics.

- Starting and Stopping Oracle Delegated Administration Services by Using the Command Line
- Starting, Stopping, and Restarting Oracle Delegated Administration Services by Using Oracle Enterprise Manager 10g Application Server Control Console
- Starting, Stopping, and Restarting Oracle Delegated Administration Services by Using the Identity Management Grid Control Plug-in

## Starting and Stopping Oracle Delegated Administration Services by Using the Command Line

To start Oracle Delegated Administration Services by using the command line, enter:

```
$ORACLE_HOME/opmn/bin/opmnctl startproc process-type=OC4J_SECURITY
```

To stop Oracle Delegated Administration Services by using the command line, enter:

```
$ORACLE_HOME/opmn/bin/opmnctl stopproc process-type=OC4J_SECURITY
```

To restart Oracle Delegated Administration Services by using the command line, enter:

```
$ORACLE_HOME/opmn/bin/opmnctl restartproc process-type=OC4J_SECURITY
```

## Starting, Stopping, and Restarting Oracle Delegated Administration Services by Using Oracle Enterprise Manager 10*g* Application Server Control Console

To start, stop, or restart Oracle Delegated Administration Services from the Oracle Enterprise Manager 10*g* Application Server Control Console:

1. Go to the standalone console for the infrastructure instance of Oracle Enterprise Manager that you want to administer. This is effected by entering the host name of the computer hosting the Oracle Application Server instance and the port number of Oracle Enterprise Manager. The default port number is `1810`, but it may be configured in increments of one, up to `1816`.

2. From the **Standalone Instances** section of the Farm page, choose the appropriate Oracle Application Server instance.
3. Select the check box next to **OC4J_SECURITY** in the System Components table and then click the **Start**, **Stop**, or **Restart** button at the top of the list.

**See Also:**

- "Task 2: Verify that Oracle Delegated Administration Services Is Running" on page 1-5
- *Oracle Internet Directory Administrator's Guide* for information on how to work with the Oracle Enterprise Manager 10*g* Application Server Control Console

## Starting, Stopping, and Restarting Oracle Delegated Administration Services by Using the Identity Management Grid Control Plug-in

You can also use the Identity Management Grid Control Plug-in to start, stop, or restart Oracle Delegated Administration Services. Refer to the *Oracle Identity Management Infrastructure Administrator's Guide* for information on using the Identity Management Grid Control Plug-in.

# 2

# Administering Oracle Delegated Administration Services

This chapter describes how to administer Oracle Delegated Administration Services. It contains these topics:

- Creating Applications by Using Oracle Delegated Administration Services
- Configuring Oracle Delegated Administration Services in an Existing Oracle Home
- Configuring Oracle Delegated Administration Services in a New Oracle Home
- Configuring Oracle Delegated Administration Services with Load Balancers in a Different DNS Domain
- Configuring Load Balancers for Multiple Instances of Oracle Delegated Administration Services
- Configuring Oracle Delegated Administration Services in a Replication Environment

## Creating Applications by Using Oracle Delegated Administration Services

You can embed Oracle Delegated Administration Services into both Oracle and third-party self-service applications that use Oracle Internet Directory. For example, if you are building a Web portal, you can add Oracle Delegated Administration Services to enable end users to change application passwords stored in the directory.

Each unit has a corresponding URL stored in the directory. To invoke a Oracle Delegated Administration Services unit, an application queries the directory at runtime for the corresponding URL.

This section contains these topics:

- Oracle Delegated Administration Services for User Entries
- Oracle Delegated Administration Services for Group Entries

> **See Also:** The chapter on the Oracle Delegated Administration Services URL API in *Oracle Internet Directory Application Developer's Guide*

### Oracle Delegated Administration Services for User Entries

Oracle Delegated Administration Services can perform these operations regarding user entries:

- Search for a user entry
- Create a user entry
- Self-edit a password
- Select a user entry and edit it
- Select a user entry and delete it
- Select a user entry and assign a privilege to that user
- View profile of the user who is logged in
- User list of values (LOV), a popup window that enables you to lookup and select a user
- Edit a user by passing the `orclguid` attribute to the URL. The entry is then displayed without the user needing to perform a search.
- Delete a user by passing the `orclguid` attribute to the URL. The entry is then displayed without the user needing to perform a search.
- Assign a privilege to a user by passing the `orclguid` attribute to the URL. The entry is then displayed without the user needing to perform a search.

### Oracle Delegated Administration Services for Group Entries

Oracle Delegated Administration Services can perform these operations regarding group entries:

- Search for a group entry
- Create a group entry
- Select a group entry and edit it
- Select a group entry and delete it
- Select a group entry and assign a privilege to that group
- Group list of values (LOV), a popup window that enables you to lookup and select a group
- Edit a group by passing the `orclguid` attribute to the URL. The entry is then displayed without the user needing to perform a search.
- Delete a group by passing the `orclguid` attribute to the URL. The entry is then displayed without the user needing to perform a search.
- Assign a privilege to a group by passing the `orclguid` attribute to the URL. The entry is then displayed without the user needing to perform a search.

## Configuring Oracle Delegated Administration Services in an Existing Oracle Home

You can use Oracle Enterprise Manager 10*g* Application Server Control Console to configure Oracle Delegated Administration Services in the Oracle Identity Management Oracle home. When you do this, Enterprise Manager:

- Sets up the URL for Oracle Delegated Administration Services
- Configures the appropriate privileges

- Deploys Oracle Delegated Administration Services in an OC4J_SECURITY instance

> **Note:** Before configuring Oracle Delegated Administration Services, ensure that Oracle Application Server Single Sign-On is configured. Configuring Oracle Application Server Single Sign-On also configures mod_osso, which is required by Oracle Delegated Administration Services. mod_osso is an Oracle HTTP Server module that communicates with the OracleAS Single Sign-On server.

To configure Oracle Delegated Administration Services by using Oracle Enterprise Manager 10*g* Application Server Control Console:

1. On the main Application Server Control Console page, select the name of the Oracle Application Server instance you want to manage in the **Standalone Instances** section. The Oracle Application Server home page opens for the selected instance.
2. Select the **Configure Components** button, located just above the System Components table. The Select Component page appears.

> **Note:** The Configure Component button is available only if you have installed but not configured any Oracle Application Server components.

3. Select **Oracle Delegated Administration Services**, then choose **Continue**. The Login page appears.
4. Enter the user name and password of the directory super user. The default user name is `cn=orcladmin`.
5. Choose **Finish** to complete the configuration.
6. Start Oracle Delegated Administration Services as follows:
   a. In the **System Components** table, select **OC4J_SECURITY** in the Name column. The OC4J_SECURITY page opens.
   b. In the **General** section, select the **Start** button.

## Configuring Oracle Delegated Administration Services in a New Oracle Home

Oracle Delegated Administration Services is configured automatically as part of the default Identity Management and Metadata Repository installation in which Oracle Internet Directory, Oracle Delegated Administration Services, and OracleAS Single Sign-On are selected. In some situations, you may need to configure it on a computer other than that on which the infrastructure is configured. You can do this in one of two ways: either by performing a standalone Oracle Delegated Administration Services installation using the Oracle Installer, or manually.

This section contains these topics:

- Performing a Standalone Oracle Delegated Administration Services Installation

## Performing a Standalone Oracle Delegated Administration Services Installation

To perform a standalone Oracle Delegated Administration Services installation, when prompted by the Oracle Installer, select the Identity Management installation type. On the Configuration Options screen, select **Delegated Administration Service**.

---

**Note:** If you configure Oracle Application Server Single Sign-On and Oracle Delegated Administration Services in separate installations against the same Oracle Internet Directory, then be sure to configure OracleAS Single Sign-On first. This is because Oracle Delegated Administration Services depends on `mod_osso`, which is not set up during installation unless the Oracle Internet Directory it points to already has OracleAS Single Sign-On configured.

---

**See Also:** *Oracle Application Server 10g Installation Guide* for further instructions

## Manually Deploying Oracle Delegated Administration Services in a New Oracle Home

To manually deploy Oracle Delegated Administration Services in a separate Oracle home, follow these steps:

1. Verify that the computer has at least a core installation that points to an existing Oracle Internet Directory and Oracle Application Server Single Sign-On.
2. Navigate to the $*ORACLE_HOME*/dcm/bin directory.
3. Create a new component by using the following command:

   ```
   dcmctl createcomponent -verbose -debug -ct oc4j -co OC4J_SECURITY
   ```

4. Start the component by using the following command:

   ```
   dcmctl start -verbose -debug -co OC4J_SECURITY
   ```

5. Deploy the `oiddas.ear` file by using the following command:

   ```
   dcmctl deployApplication -debug -verbose -a oiddas -f
   $ORACLE_HOME/ldap/das/oiddas.ear -co OC4J_SECURITY
   ```

6. Perform the following steps to add the `LD_LIBRARY_PATH` and `DISPLAY` environment variables to the opmn.xml file:

   a. Navigate to the $*ORACLE_HOME*/opmn/conf directory and open opmn.xml in a text editor.

   b. Add the following lines in the OC4J_SECURITY section of opmn.xml:

   **For a UNIX environment:**

   ```
   <environment>
   <prop name="LD_LIBRARY_PATH" value="%ORACLE_HOME%/lib"/>
   </environment>
   ```

   **For a Windows environment:**

   ```
   <environment>
   ```

```
<prop name="PATH" value="%ORACLE_HOME%/bin"/>
</environment>
```

Note the placement of the section `<environment>` in the following example.

```
<oc4j maxRetry="3" instanceName="OC4J_DAS" gid="OC4J_SECURITY"
numProcs="1">
<config-file path="/home/ias902/j2ee/OC4J_
DAS/config/server.xml"/>
<oc4j-option value="-properties"/>
<port ajp="3001-3100" jms="3201-3300"
rmi="3101-3200"/>
<environment>
<prop name="LD_LIBRARY_PATH" value="/home/ias902/lib"/>
</environment>
</oc4j>
```

**c.** Navigate to the $*ORACLE_HOME*/dcm/bin directory.

**d.** Save the changes to the repository by using the following command:

```
dcmctl updateconfig -verbose -debug -ct opmn
```

**e.** Restart OPMN by using the following command:

```
dcmctl restart -verbose -ct opmn
```

**f.** Stop and start the OC4J_SECURITY instance by using the following commands:

```
dcmctl stop -verbose -debug -ct oc4j -co OC4J_SECURITY
dcmctl start -verbose -debug -ct oc4j -co OC4J_SECURITY
```

**g.** Set the necessary permissions for Oracle Delegated Administration Services. Modify the group by using either Oracle Directory Manager or the command-line tool. Add the DN of the new Oracle Application Server instance where Oracle Delegated Administration Services is currently being deployed as the `uniquemember`.

```
DN of the group to be modified:
cn=Associated
Mid-tiers,orclApplicationCommonName=DASApp,cn=DAS,cn=Products,cn=OracleCont
ext
```

The DN on the Oracle Application Server instance is:

```
orclApplicationCommonName=name of Oracle Application Server instance,cn=IAS
Instances, cn=IAS, cn=Products,
cn=OracleContext
```

where *`name of Oracle Application Server instance`* is obtained from $*ORACLE_HOME*/config/ias.properties.

# Configuring Oracle Delegated Administration Services with Load Balancers in a Different DNS Domain

When configuring Oracle Delegated Administration Services in an environment where Oracle Application Server Single Sign-On is to be configured on separate middle tier nodes, follow the instructions on advanced configurations in the *Oracle Application Server Single Sign-On Administrator's Guide*.

## Configuring Load Balancers for Multiple Instances of Oracle Delegated Administration Services

Because Oracle Delegated Administration Services is a stateful application, if you deploy multiple instances of Oracle Delegated Administration Services behind a load balancer, then the load balancer must be configured to support session binding in order to maintain a consistent user experience. Session binding refers to a user session being bound to an origin server in order to maintain state for a specified period of time. In other words, you should configure the load balancer so it routes all requests for each user to the same Oracle Delegated Administration Services middle tier.

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

## Configuring Oracle Delegated Administration Services in a Replication Environment

To configure Oracle Delegated Administration Services and Oracle Application Server Single Sign-On for a replication environment, follow these steps:

1. Navigate to the $*ORACLE_HOME*/config folder and open the ias.properties file in a text editor.
2. Change the value assigned to the `DAS.LaunchSuccess` parameter from `true` to `false`.
3. Restart Oracle Delegated Administration Services by following the procedures described in Starting and Stopping Oracle Delegated Administration Services on page 1-7.

# Part II

# Oracle Internet Directory Self-Service Console

This part explains how users can work with the Oracle Internet Directory Self-Service Console, including how to search for entries and manage their own profiles. This part also includes information on how to manage users and groups with the Oracle Internet Directory Self-Service Console.

Part II contains the following chapters:

# 3

# Working with the Oracle Internet Directory Self-Service Console

The following topics describes how to use the Oracle Internet Directory Self-Service Console:

- Getting Started with the Self-Service Console
- Searching for Entries by Using the Self-Service Console

## Getting Started with the Self-Service Console

This section explains how to start, log in to, and stop the Self-Service Console. It contains these topics:

- Starting and Stopping the Oracle Internet Directory Self-Service Console
- Logging into the Oracle Internet Directory Self-Service Console

### Starting and Stopping the Oracle Internet Directory Self-Service Console

To use the Self-Service Console, you need to start the Oracle Delegated Administration Services by following the procedures described in "Starting and Stopping Oracle Delegated Administration Services" on page 1-7.

### Logging into the Oracle Internet Directory Self-Service Console

To log in to the Self-Service Console:

1. Visit the URL of the Self-Service Console. For example, if the Self-Service Console is installed on `host1.acme.com` and the Oracle HTTP Server is running on port 7778, then the URL to the Self-Service Console is http://host1.acme.com:7778/oiddas/.
2. In the upper right corner, select **Login**. This takes you to the Oracle Application Server Single Sign-On window.
3. In the Single Sign-On window, in the **User Name** field, enter your Self-Service Console user name--for example, `jdoe`.
4. In the **Password** field, enter your Self-Service Console password.
5. If you are in a hosted environment in which there are multiple hosted companies, then the **Company** field appears. Otherwise, it does not appear. If the **Company** field appears, then enter the name of your company.
6. Choose **Login**.

# Searching for Entries by Using the Self-Service Console

This section explains how to use the Self-Service Console to search for user and group entries, perform advanced searches, and search for uses that match specified provisioning criteria. It contains these topics:

- Searching for User Entries by Using the Self-Service Console
- Searching for Group Entries by Using the Self-Service Console
- Performing an Advanced Search

> **See Also:** "Missing User Entries" on page B-7 if user entries that exist in Oracle Internet Directory do not appear when you search for them in the Self-Service Console

## Searching for User Entries by Using the Self-Service Console

To search for user entries:

1. In the Oracle Internet Directory Self-Service Console, select the **Directory** tab, then select **Users**. The Search for Users window appears.

   This window is described in "Search for Users" on page A-24.

2. In the **Search for User** field, enter the first few characters of one of the following:
   - E-mail address
   - First name
   - Last name
   - User ID

   For example, if you are searching for Anne Smith, you could enter `Ann` or `Smi`.

   To generate a list of all users in the directory, leave this field blank.

3. Choose **Go** to display the search results.

## Searching for Group Entries by Using the Self-Service Console

To search for a group entry:

1. Select the **Directory** tab, then select **Groups**. The Search for Groups window appears.

   This window is described in "Search for Groups" on page A-24.

2. In the **Search Group Name** text box, enter the first few characters of the name of the group for which you are searching.

   To generate a list of all groups in the directory, leave this field blank.

3. Choose **Go** to display the entries that match the criteria you entered.

## Performing an Advanced Search

To perform an advanced search:

1. Select the **Directory** tab, then select **Users**. From the Users page, click **Advanced Search**. The Advanced Search window appears.

   This window is described in "Advanced Search" on page A-4.

2. Select one of the following options to determine how you want to search for users:
   - **Find users that match all conditions**
   - **Find users that match any condition**
3. For each of the attributes you want to search, select one of the following conditions from the box next to each attribute name:
   - **is (default)**
   - **is not**
   - **is present**
   - **is not present**
   - **contains**
   - **does not contain**
   - **starts with**
   - **ends with**
4. Enter the first few characters for which you are searching in the text boxes for any of the following attributes:
   - **E-mail address**
   - **First name**
   - **Last name**
   - **User ID**
5. To add additional search attributes, select an attribute name from the **Add Another** box, then click **Add**.
6. Choose **Go** to display the entries that match the criteria you entered.

# 4

# Managing Your Profile with the Oracle Internet Directory Self-Service Console

The following topics explains how to manage elements in your personal profile, including password, photo, time zone, organizational chart, and resource access information:

- Viewing Your Profile
- Editing Your Profile
- Changing Your Own Password and Password Hint
- Resetting Your Password If You Forget It
- Viewing Your Organizational Chart
- Changing Your Time Zone Setting
- Managing Your Own Resource Information

## Viewing Your Profile

To view your profile, select the **My Profile** tab, then choose **View My Profile**. The View My Profile window appears.

This window is described in "View My Profile" on page A-25.

> **Note:** To refresh this window with the latest information in the server, choose Refresh My Profile. Do not use the refresh or reload button on your browser, which simply refreshes with information from the mid-tier cache and not from the server.

## Editing Your Profile

To edit your profile:

1. Select the **My Profile** tab, then choose **Edit My Profile**. The Edit My Profile window appears.

   This window is described in "Edit My Profile" on page A-17.

2. Make your changes.
3. Choose **Submit**.

# Changing Your Own Password and Password Hint

You can use the Self-Service Console to change your own password to OracleAS Single Sign-On and other Oracle components. Changing your password for OracleAS Single Sign-On also changes your password for any applications that use OracleAS Single Sign-On for authentication.

To change your password, select the **My Profile** tab, then select **Manage My Password**. The Manage Password window appears. You can use this window to change your password to either OracleAS Single Sign-On or to another Oracle component.

This window is described in "Manage Password" on page A-22.

To change your password to Oracle Application Server Single Sign-On:

1. In the **Single Sign-On Password** section, in the **Old Password** field, enter your current password.
2. In the **New Password** field, enter your new password, then confirm it by entering it again in the **Confirm New Password** field.
3. In the **Password Reset** section, in the **Password Reset Hint** field, enter a question—for example, your mother's maiden name. If you later forget your password, then you will be asked this question. If your answer is correct, then your password will be retrieved for you.
4. In the **Answer to Password Reset Hint** field, enter the answer to the hint you just entered in the previous field.
5. Choose **Submit**.

> **Note:** When you enter an answer to your password hint in the Answer to Password Hint field, be sure to remember the answer exactly as you entered it. Any deviation—for example, extra spaces, additional hyphens, or capitalizations—causes the hint answer not to match the stored version.

To change your password to another Oracle component that is not enabled for Oracle Application Server Single Sign-On:

1. In the **Application Passwords** section, select the Oracle component for which you want to specify a new password.
2. Choose **Update Password**. The Change Application Password window appears.

   This window is described in "Change Application Password" on page A-11.
3. In the **New Password** field, enter your new password, then confirm it in the **Confirm New Password** field.
4. Choose **Submit**.

# Resetting Your Password If You Forget It

If you forget your password, you can reset it. For security reasons, this requires you to answer the question you specified when you first established your password.

1. In the Self-Service Console home page, choose **Forgot Your Password**. The Reset My Single Sign-On Password window appears.

This window is described in "Reset My Single Sign-On Password" on page A-23.

2. In the **Confirm Identity** section, enter values for the fields. These fields are specific to your environment and are configured by the administrator. You must also enter the name of your company.
3. Choose **Next**. The Confirm Additional Personal Information window appears.

   This window is described in "Confirm Additional Personal Information" on page A-12.
4. If, in "Changing Your Own Password and Password Hint" on page 4-2, you set your password hint, then the Confirm Additional Personal Information window asks you a question based on that hint. Enter the answer to the password hint you specified.

   If you did not previously set a password hint, then the Confirm Additional Personal Information window prompts you for other personal data as configured by your administrator. This data is then used to validate your identity.
5. Choose **Next**. The Reset SSO Password window appears.

   This window is described in "Reset SSO Password" on page A-23.
6. In the **New Password** field, enter your new password, then confirm it by entering it again in the **Confirm New Password** field.
7. Choose **Submit**.

## Viewing Your Organizational Chart

The Self-Service Console includes an organization chart that displays your organization's hierarchy. The hierarchy is created automatically according to each employee's manager and title.

To locate yourself within the hierarchy of your organization, select the **My Profile** tab, then select **View My Org Chart**. To locate another employee within the hierarchy of your organization, perform the following steps:

1. Search for an employee by following the instructions described in "Searching for Entries by Using the Self-Service Console" on page 3-2.
2. Click the employee's **Job Title** link to display the Organization Chart window.

   This window is described in "Organization Chart" on page A-22.

The organization chart displays in a table that enables you to expand and collapse the entries beneath each manager. The organizational chart includes the following entries:

- All managers above the currently selected employee
- All peers of the currently selected employee
- All employees who report to the currently selected employee

You can view a employee's profile by clicking his or her name in the organizational chart. You can also navigate the organizational hierarchy by clicking an employee's **Job Title** link.

## Changing Your Time Zone Setting

To change your time zone setting this:

1. Select the **My Profile** tab, then select **Change My Time Zone**. This takes you to the Time Zone Settings window.

   This window is described in "Time Zone Settings" on page A-24.

2. In the Time Zones Settings window, select your new time zone, then choose **Submit**.

# Managing Your Own Resource Information

To fulfill the requests of users, some Oracle components gather data from various repositories and services. To gather the data, these components require the following information:

- Information specifying the type of resource from which the data is to be gathered. The type of resource could be, for example, an Oracle Database. This is called resource type information.
- Information for connecting and authenticating users to the resources. This is called resource access information.

You can use the Self-Service Console to create, modify, and delete resource access information, as described in the following topics.

- Creating Resource Access Information
- Modifying Resource Access Information
- Deleting Resource Access Information

> **Note:** The **Preferences** link mentioned in this section appears only if the administrator has created resource access information for the user.

You can manage your own resource access information only if the administrator has specified a resource type. If a resource type has been specified, then a Preferences link appears.

## Creating Resource Access Information

To specify resource access information:

1. Select the **My Profile** tab, then choose **Preferences**.
2. Choose **Create**. The Create Resource window appears.

   This window is described in "Create Resource" on page A-15.

3. In the **Resource Name** field, specify the name of the resource or service to be accessed by the component on your behalf.
4. From the **Resource Type** list, select the type of resource to be accessed. Default options are:
   - **OracleDB**: Oracle Database 10*g*
   - **ExpressPDS**: Oracle Express Pluggable Data Source
   - **JDBCPDS**: Java Database Connectivity Pluggable Data Source

   Other resource types may appear in this list as specified by the administrator.
5. Choose **Next**. The Resource Access Information window appears

This window is described in "Resource Access Information" on page A-24.

6. In the Resource Access Information window, enter the appropriate information.
7. Choose **Submit**.

## Modifying Resource Access Information

To modify resource access information:

1. Select the **My Profile** tab, then choose **Preferences**.
2. Select the resource whose information you want to modify, then choose **Edit**. The Edit Resource window appears.

   This window is described in "Edit Resource" on page A-18.
3. In the Edit Resource window, enter the appropriate information.
4. Choose **Submit**.

## Deleting Resource Access Information

To delete resource access information:

1. Select the **My Profile** tab, then choose **Preferences**.
2. Select the resource whose information you want to delete.
3. Choose **Delete**. The Delete Resource window appears.

   This window is described in "Delete Resource" on page A-17.
4. Click **Yes** to delete the resource or **No** to return to the Preferences page.

> **See Also:** The section on resource information in the Concepts and Architecture chapter of the *Oracle Internet Directory Administrator's Guide* for a brief description of resource information

# 5

# Managing Users and Groups with the Oracle Internet Directory Self-Service Console

The following topics describe how to manage users and groups with the Oracle Internet Directory Self-Service Console:

- About the Oracle Internet Directory Self-Service Console
- Managing Identity Management Realms
- Managing User Entries
- Managing Group Entries
- Managing Services
- Managing Accounts
- Managing Resource Information

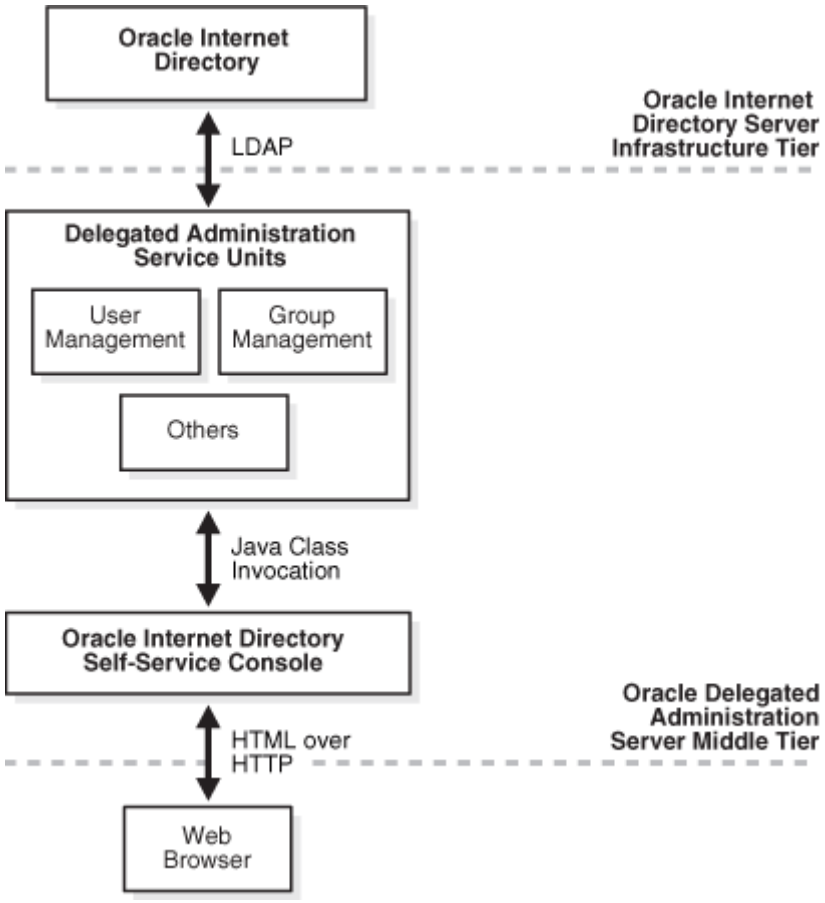
> **See Also:** *Oracle Identity Management Integration Guide* for information on provisioning with the Oracle Internet Directory Provisioning Console

## About the Oracle Internet Directory Self-Service Console

The Oracle Internet Directory Self-Service Console enables you to delegate administrative privileges to various administrators and to end users. It is a ready-to-use standalone application created by using Oracle Delegated Administration Services. It provides a single graphical interface for delegated administrators and end users to manage data in the directory.

Figure 5–1 shows how the Self-Service Console interacts with Oracle Delegated Administration Services.

*Figure 5–1 Interactions of Oracle Internet Directory Self-Service Console with Oracle Delegated Administration Services*




# Managing Identity Management Realms

This section explains how to use the Self-Service Console to configure a realm, modify those configurations, and create additional realms. It contains these topics:

- Configuring an Identity Management Realm
- Configuring the Parent DN for Entries in a Realm
- Creating an Additional Identity Management Realm
- Viewing Configuration Settings for Additional Identity Management Realms

## Configuring an Identity Management Realm

If you have the correct administrative privileges, then you can specify the following for an identity management realm:

- The attribute by which you want users to identify themselves when they log in
- The root entries of the user search base and of the group search base—that is, the locations in the directory information tree containing entries for users and groups
- The root entries for the user creation base and the group creation base—that is, the location in the DIT where users and groups are created. This can be the same as the user search base or a location under the user search base.

- The display of realm and product logos

> **Note:** Any changes you make to an identity management realm will only affect the realm which you are currently logged into as an administrator. In other words, changes you make to one realm are not automatically propagated to other realms.

To configure an identity management realm:

1. Log in with the administrator account for the realm you want to configure.
2. Select the **Configuration** tab, then choose **Identity Management Realm**. The Identity Management Realm Configuration window appears.

   This window is described in "Identity Management Realm Configuration" on page A-20.
3. In the Identity Management Realm window, enter values for the various fields.
4. Choose **Submit** to save your changes.

> **Note:** Although you can enter more than one value in the **User Search Base** field, doing so can degrade performance.

## Configuring the Parent DN for Entries in a Realm

You can specify one or more parent DNs for entries in a realm. If you specify more than one, then a delegated administrator can choose the one under which to place a new user entry.

There are two ways to specify parent DNs. The first is by specifying values for the User Creation Base, and the second is by specifying values for the organizational units (`ou`) attribute. If you specify a different set of values for each, then those for the `ou` attribute prevail.

> **Note:** When you add new values to the User Creation Base or organizational units, you must ensure that the containers exist in Oracle Internet Directory and that the access controls are properly configured. See *Oracle Internet Directory Administrator's Guide* for information on how to set up access controls for the User Creation Base or organizational units.

To specify parent DNs by providing values for the User Creation Base:

1. Select the **Configuration** tab, then choose **Identity Management Realm**. The Identity Management Realm Configuration window appears.

   This window is described in "Identity Management Realm Configuration" on page A-20.
2. In the **User Creation Base** field, enter one or more DNs, one line for each DN.
3. Choose **Submit**.

Alternatively, you can specify parent DNs by setting the value for the organizational unit (`ou`) attribute. If you do this, then a delegated administrator can choose the

organization unit under which to place user entries. To specify a parent DN by using this method:

1. Select the **Configuration** tab, then choose **User Entry**. The Configure User Object Classes window appears.

   This window is described in "Configure User Object Classes" on page A-12.

2. Choose **Next**. The Configure User Attributes window appears.

   This window is described in "Configure User Attributes" on page A-12.

3. Choose **Add New Attribute**. The Add/Edit Attribute window appears.

   This window is described in "Add/Edit Attribute" on page A-3.

4. In the Add New Attributes window, from the **Directory Attribute Name** list, select the `ou` attribute.

5. From the **UI Type** list, select **Predefined List**.

6. In the **LOV Values** field, enter the display name of the parent DN, followed by three semicolons (;), followed by the DN itself.

   For example:

   ```
   Sales;;;cn=users,dc=us,dc=my_company,dc=com
   HR;;;cn=groups,dc=us,dc=my_company,dc=com
   ```

   Following this example, when a delegated administrator chooses the organizational unit under which to place a user entry, she selects from a list displaying `Sales` and `HR`.

   You can add more parents DNs, one line for each.

7. Choose **Done**.

## Creating an Additional Identity Management Realm

If you have the administrative privileges, then you create an entry for an identity management realm as follows:

1. Select the Configuration tab.

   At the top right of the Oracle Internet Directory Self Service Console, choose the **Realm Management** icon. The Identity Management Realms window appears.

   This window is described in "Identity Management Realms" on page A-21.

2. In the Identity Management Realms window, choose **Create**. The Create Identity Management Realm window appears.

   This window is described in "Create Identity Management Realm" on page A-14.

3. In the Create Identity Management Realm window, enter the appropriate values in the fields.

4. Choose **Submit**.

## Viewing Configuration Settings for Additional Identity Management Realms

To view the configuration settings of an identity management realm:

1. Select the Configuration tab.

2. At the top right of the Self-Service Console, choose the **Realm Management** icon. The Identity Management Realms window appears.

This window is described in "Identity Management Realms" on page A-21

3. In the Identity Management Realms window, in the **Search Identity Management Realm** field, enter all or part of the name of the realm whose entry you want to view, then choose **Go**. This displays a list of realms that match your search criteria.
4. From the search results list, select the realm you want to view, then choose View. This takes you to the View Identity Management Realm window where you can view the configuration settings.

   This window is described in "View Identity Management Realm" on page A-25.

# Managing User Entries

This section explains how to use the Self-Service Console to manage user entries. It contains these topics:

- Configuring User Entries
- Viewing User Entries
- Creating User Entries
- Modifying User Entries
- Deleting User Entries
- Managing Users in Bulk
- Assigning Privileges to Users
- Changing the Password of a User
- Specifying Additional Password Reset Validation Questions

## Configuring User Entries

When a user creates or edits a user entry, the Self-Service Console displays various categories—including, for example, basic information, password, and photo—each with its own set of attributes. You can specify which of these categories the console displays, and how it displays them and their corresponding attributes.

Specifically, the Self-Service Console enables you to:

- Select from object classes now in the directory those you want to associate with user entries, and add and modify these object classes
- Specify the categories of attributes you want to enable users to add or modify
- Customize the way the Self-Service Console displays those categories and attributes

> **See Also:** *Oracle Internet Directory Administrator's Guide* for information on how to administer Oracle Internet Directory object classes and attributes

To configure user entries:

1. Select the **Configuration** tab, then select **User Entry**. This displays the Configure User Object Classes window listing the existing object classes associated with user entries.

   This window is described in "Configure User Object Classes" on page A-12.

2. To add an object class for user entries:

   a. In the Configure User Object Classes window, choose **Add Object Class**. The All Object Classes window appears.

      This window is described in "All Object Classes" on page A-5.

   b. Select from the list an object class you want to add, then choose **Add**. This returns you to the Configure Object Class window. The object class you just chose is now listed as an object class for user entries.

   c. To add more object classes, repeat these steps, or, to move to the next step, choose **Next** to display the Configure User Attributes window.

      This window is described in "Configure User Attributes" on page A-12.

3. The Configure User Attributes window lists some—but not all—of the attributes of the object classes you specified in Step 2 on page 5-6. There may be other attributes belonging to those object classes as well. You can add as many of those other attributes as you wish by following the instructions in this step. You can modify how the attributes are displayed or delete attributes.

   To add attributes to user entries:

   a. In the Configure User Attributes window, choose **Add New Attribute**. The Add/Edit Attribute window appears.

      This window is described in "Add/Edit Attribute" on page A-3.

   b. In the Add New Attribute window, enter values for the fields.

   c. Choose **Done**. This returns you to the Configure User Attributes window. The attribute you just chose is now listed in the attribute list.

   d. To add more attributes, repeat these steps.

   To modify the display of attributes:

   a. In the Configure User Attributes window, in the **Directory Attribute Name** column, select the attribute you want to modify, then choose **Edit**. The Editing Attribute window appears.

      This window is described in "Editing Attribute" on page A-18.

   b. In the Editing Attribute window, enter values for the fields.

   c. Choose **Done**. This returns you to the Configure User Attributes window. The attribute configurations you just made are now reflected in the Directory Attribute Name list.

   d. To configure or modify more attributes, repeat these steps.

   To delete attributes of user entries, in the Configure User Attributes window, in the **Directory Attribute Name** list, select the attribute you want to configure, then choose **Delete**.

4. To customize the display of categories, in the Configure User Attributes window choose **Next** to display the Configure Attribute Categories window, which contains a table listing the existing categories, the name displayed to the user, and the display order of each category.

   This window is described in "Configure Attribute Categories" on page A-12.

   a. To add a new category, choose **Create**. The Create window appears. In the **UI Label** field, enter the name of the category as you would like it displayed in the interface.

b. To modify the display name of a category, in the **UI Label** column, edit the field for each attribute you want to modify.

c. To set the display order of categories, choose **Order Category** to display the Order Category window displays the various categories you just specified.

This window is described in "Order Category" on page A-22.

d. To set the display order of attributes for each category, select the category, then choose **Edit** to display the Edit Category window.

This window is described in "Edit Category" on page A-17.

e. To delete a category, select the category, then choose **Delete** to display the Delete Category window. Click **Yes** to delete the category or **No** to return to the Configure Attribute Categories page.

This window is described in "Delete Category" on page A-17.

When you have finished configuring attribute categories, choose **Next** to display the Configure Search Table Columns window.

This window is described in "Configure Search Table Columns" on page A-12.

5. When a user performs a search, the results are displayed in a table. You can specify the number of columns in that table and their headings. To configure search table columns:

a. In the Configure Search Table Column window, in the **All Attributes** box, select one or more attributes that you want to be represented in the search results. These will serve as column headings in the search results table.

b. Use the left-right arrows to move the attributes to the **Selected Attributes** box.

c. In the **Selected Attributes** box, order the attributes by using the up-down arrows to the right of the box. The first attribute in the list represents the column farthest to the left in the search results table.

When you have finished configuring the search results table, choose **Next** to display the Configure Roles window.

This window is described in "Configure Roles" on page A-12.

6. To enable users to assign roles to users, in the Configure Roles window, in the **Enable Roles** category, select Enable Role assignment in the user management interface.

You can specify the roles that users can assign to other users.

To add a role that users can assign to other users:

a. Choose **Add Role** to display the Search and Select: Roles window.

b. In the **Group Name Begins With** field, enter the first few letters of the name of the administrative group you want to add.

c. From the search results, select the name of the administrative group you want to add, then choose **Select**. This returns you to the Configure Roles window. The administrative group you just selected appears in the Roles list.

To delete a role, select it from the table and choose **Delete**.

7. When you have finished configuring user entries, choose **Finish**.

## Viewing User Entries

To view a user entry:

1. Search for a user entry by following the instructions described in "Searching for Entries by Using the Self-Service Console" on page 3-2.
2. Select the user whose entry you want to view, then click the **View** button to display the View User window.

   This window is described in "View User" on page A-25.

## Creating User Entries

To create a user entry:

1. Select the **Directory** tab, then select **User**.
2. Choose **Create** to display the Create User window.

   This window is described in "Create User" on page A-16.
3. In the Create User window, enter the appropriate information. Fields designated with an asterisk (*) are mandatory.

   **Caution:** The User ID field cannot contain spaces or any of the following characters: " ( ) * + , ; < > \ ~ & ' % ? / = ^ | ~

   If resource access information is not specified, you can create it. To do this:

   a. In the **Resource Access Information** section, choose **Create** to display Create Resource window.

      This window is described in "Create Resource" on page A-15 window.

   b. In the **Resource Name** field, specify the name of the resource or service to be accessed by the component on your behalf.

   c. From the **Resource Type** list, select the type of resource to be accessed. Default options are:

      * **OracleDB**: Oracle Database 10*g*
      * **ExpressPDS**: Oracle Express Pluggable Data Source
      * **JDBCPDS**: Java Database Connectivity Pluggable Data Source

      Other resource types may appear in this list as specified by the administrator.

   d. Choose **Next**. The Resource Access Information window appears.

   e. In the Resource Access Information window, specify the user name and password and the name of the database that you want the user to access.

   f. Verify that you have entered all information correctly, then choose **Submit**.

## Modifying User Entries

To modify a user entry:

1. Select the **Directory** tab, and perform a search for the user whose entry you want to modify.

2. Select the user whose entry you want to modify, then choose **Edit** to display the **Edit User** window.

   This window is described in "Edit User" on page A-18.

3. In the Edit User window, enter the appropriate information. Fields designated with an asterisk (*) are mandatory. If resource access information is not specified, you can create it. To do this:

   a. In the **Resource Access Information** section, choose **Create**. The Create Resource window appears.

   b. In the **Resource Name** field, specify the name of the resource or service to be accessed by the component on your behalf.

   c. From the **Resource Type** list, select the type of resource to be accessed. Default options are:

      * **OracleDB**: Oracle Database 10*g*
      * **ExpressPDS**: Oracle Express Pluggable Data Source
      * **JDBCPDS**: Java Database Connectivity Pluggable Data Source

      Other resource types may appear in this list as specified by the administrator.

   d. Choose **Next**. The Resource Access Information window appears.

   e. In the Resource Access Information window, specify the user name and password and the name of the database that you want the user to access.

   f. Verify that you have entered all information correctly, then choose **Submit**.

---

**Note:** If you do not have the privileges to edit a user entry, then the **Edit** button does not appear, and you cannot perform this operation.

---

## Deleting User Entries

To delete a user entry:

1. Search for the user you want to delete by following the instructions in "Searching for Entries by Using the Self-Service Console" on page 3-2.

2. Select the user you want to delete from the search results table, then click **Delete**. The Delete User window appears and prompts you to confirm deletion.

   This window is described in "Delete User" on page A-17.

3. In the Delete User window, click **Yes** to delete the user or **No** to return to the Users page.

## Managing Users in Bulk

You can upload an LDIF (LDAP Data Interchange Format) file to the Provisioning Console to create, edit, or delete users in bulk mode.

To create, edit, or delete users in bulk mode:

1. Select the **Directory** tab, then select **User**.

2. Choose **Bulk** to display Bulk User Management window.

   This window is described in "Bulk User Management" on page A-11.

3. In the Bulk User Management window, choose **Browse** to locate the LDIF file containing the data for the users you want to create, edit, or delete.
4. To ignore failed users, select the **Ignore Failed Users** box. If you select the Ignore Failed Users box, the bulk create process will attempt to create, edit, or delete users regardless of failures. Failed users will be placed in a file you can download at the end of the process. If you do not select the Ignore Failed Users box, the bulk management process will terminate at the first failed user.
5. Choose **OK**.

## Assigning Privileges to Users

You can privilege a user to:

- Create, edit, and delete users and groups
- Assign privileges to other users and groups

You can also revoke privileges from a user.

To assign privileges to a user:

1. Search for the user entry to which you want to assign privileges by following the instructions described in "Searching for Entries by Using the Self-Service Console" on page 3-2.
2. From the search results list, select the user to whom you want to assign privileges, then choose **Privileges**. The Assign Privileges to User window displays a list of privileges.

   This window is described in "Assign Privileges to User" on page A-10.
3. Select the privileges you want to assign to this user.
4. Choose **Submit**.

---

**Note:** Any changes you make to a user's privileges will not take effect until the user logs out and logs back into the Self-Service Console.

---

## Changing the Password of a User

You can change the password of a user other than yourself if:

- You have the necessary access rights
- You have configured user entries so that the `userpassword` attribute is available for modification. The steps for specifying a user attribute for modification are described in "Configuring User Entries" on page 5-5.

To change another user's password, following the instructions in "Creating User Entries" on page 5-8.

## Specifying Additional Password Reset Validation Questions

The Self-Service Console allows users to specify a custom password hint that the user must successfully answer before a password is reset. Additionally, an administrator can specify an unlimited number of questions that a user must successfully answer before a password is reset.

**See Also:** "Changing Your Own Password and Password Hint" on page 4-2

To specify additional password reset validation questions:

1. Use Oracle Directory Manager to perform the following tasks:
   a. Add custom attributes to the directory schema. You should create a separate attribute for each password reset validation question.
   b. Create a new auxiliary object class and assign to it the custom attributes you created in the last step that represent each password reset validation question.

      **See Also:** *Oracle Internet Directory Administrator's Guide* for information on how to administer Oracle Internet Directory object classes and attributes

2. To make the new object class and attributes you created in Step 1 available, select the **Configuration** tab, then select **User Entry**. This displays the Configure User Object Classes window listing the existing object classes associated with user entries. Click **Refresh Page** new object class and attributes available.

   This window is described in "Configure User Object Classes" on page A-12.

3. Add the new object class and attributes by following the procedures described in "Configuring User Entries" on page 5-5. In the Configure User Attributes window, be sure to select the **Viewable** and **Password Reset Validation** check boxes for each attribute that represents a password reset validation question. You can also select the **Self Editable** check box if you want to give users the ability to edit an attribute.

# Managing Group Entries

This section explains how to use the Self-Service Console to create, modify, and delete group entries and to assign privileges to groups. It contains these topics:

- Viewing Group Entries
- Creating Group Entries
- Modifying Group Entries
- Deleting Group Entries
- Assigning Privileges to Groups

## Viewing Group Entries

To view a group entry:

1. Select the **Directory** tab, then select **Group**.
2. Search for the group entry you want to view by following the instructions described in "Searching for Group Entries by Using the Self-Service Console" on page 3-2.
3. From the search results, click name of the group entry you want to view. The View Group window appears.

   This window is described in "View Group" on page A-25.

## Creating Group Entries

To create a group entry:

1. Select the **Directory** tab, then select **Group**.
2. Choose **Create**. The Create Group window appears.

   This window is described in "Create Group" on page A-13.
3. In the Create Group window, enter the values for the various fields.
4. Choose Submit.

## Modifying Group Entries

To modify a group entry:

1. Search for the group entry you want to modify by following the instructions described in "Searching for Group Entries by Using the Self-Service Console" on page 3-2.
2. From the search results, select the group entry you want to modify.
3. Choose **View/Manage**. The Manage Group window appears.

   This window is described in "Manage Group" on page A-22.
4. Choose **Edit**. The Edit Group window appears.

   This window is described in "Edit Group" on page A-17.
5. In the Edit Group window, modify the fields as necessary.
6. Choose **Submit**.

## Deleting Group Entries

To delete group entries:

1. Search for the group entry you want to delete by following the instructions described in "Searching for Group Entries by Using the Self-Service Console" on page 3-2.
2. From the search results, select the group whose entry you want to delete.
3. Choose View/Manage. The Manage Group window appears.

   This window is described in "Manage Group" on page A-22.
4. In the Manage Group window, choose **Delete**. The Confirmation of Deletion window appears.

   This window is described in "Confirmation of Deletion" on page A-13.
5. In the Confirmation window, choose either Yes or No.

## Assigning Privileges to Groups

You can privilege a group to do one or more of the following:

- Create, edit, and delete new users and groups
- Assign privileges to users and to other groups

You can also revoke privileges from a group.

To assign privileges to a group:

1. Search for the group entry to which you want to assign privileges by following the instructions described in "Searching for Group Entries by Using the Self-Service Console" on page 3-2.
2. From the search results, select the group to which you want to assign privileges.
3. Choose **Assign Privilege**. The Assign Privileges to Group window displays a list of privileges.

   This window is described in "Assign Privileges to Group" on page A-10.
4. In the Assign Privileges to Group window, select the privileges you want to assign to this group.
5. Choose **Submit**.

# Managing Services

This section explains how to use the Self-Service Console to modify service properties and modify subscription information for service recipients. It contains these topics:

- About Services and Delegated Administration
- Modifying Service Properties
- Modifying Subscription Information for a Service Recipient

> **Note:** You cannot configure or manage custom application services with the Self-Service Console.

## About Services and Delegated Administration

A service can be a single application or a bundle of applications that performs a coherent set of tasks. It is supplied by a service provider to either individuals or groups, called service recipients.

To access a service, a service recipient must be subscribed to it. In the subscription process, an administrator for either a subscriber or a service provider creates a subscription list. This list specifies which service recipient users can use the service and for how long.

Service recipients can be service providers in their own right, supplying services to other service recipients.

The administrative tasks you can perform with the Self-Service Console depend on whether you are an administrator for a subscriber or for a service provider. If you are an administrator for a subscriber, then you can:

- Modify the entry for your subscriber
- Create, modify, and delete subscription information for a service. For example, you can specify how long a user can use a service, then change or delete that information.
- Manage the subscription list

If you are the administrator for a service provider, then, in addition to performing all of the tasks of an subscriber administrator, you can:

- Create entries for subscribers
- Provision applications and services in the application service provider environment

## Modifying Service Properties

You can change the display name and the network address for a service. To do this:

1. Select the **Directory** tab, then select **Services**. The Services window displays a list of available services.

   This window is described in "Services" on page A-24.

2. In the Services window, select the service whose properties you want to modify.
3. Choose **Edit Service**. The Edit Service window appears.

   This window is described in "Edit Service" on page A-18.

4. In the Edit Service window, enter values for the fields you want to modify.
5. Choose **Submit**.

## Modifying Subscription Information for a Service Recipient

You can add or remove a user from a subscription list. You can also change a recipient's start or end date.

To modify subscription information:

1. Select the **Directory** tab, then select **Service**. The Services window displays a list of available services.

   This window is described in "Services" on page A-24.

2. In the Services window, select the service whose properties you want to modify.
3. Choose **Edit Subscription**. The Edit Subscription window appears.

   This window is described in "Edit Subscription" on page A-18.

4. Select the service recipient whose subscription information you want to modify.
5. Choose **Edit**. The Edit Service Recipient window appears.

   This window is described in "Edit Service Recipient" on page A-18.

6. In the Edit Service Recipient window, enter your modifications:

   a. In the **Start Date** field, specify the date on which the recipient can begin using the service.

   b. In the **End Date** field, specify the date on which that usage ends.

   To add users to the subscription list:

   a. Choose **Add User**. The Search and Select window appears.

      This window is described in "Search and Select" on page A-24.

   b. In the Search and Select window, perform a search for the user you want to add to the list.

   c. From the search results, select the user you want to add, then choose **Select**. This returns you to the Add New Service recipient window. The user you just added now appears in the list.

   To remove a user from the subscription list, select the user, then choose **Remove User**.

7. When you have made your changes in the Edit Service Recipient window, choose **Submit**. This returns you to the Edit Subscription window.

**Note:** The format of the date is `mm/dd/yyyy`. This format cannot be customized.

# Managing Accounts

This section explains how to use the Self-Service Console to unlock, enable, or disable user accounts. It contains these topics:

- Unlocking User Accounts
- Enabling User Accounts
- Disabling User Accounts

## Unlocking User Accounts

If a user's account has been locked for any reason—for example, they failed to change their password within the specified time limit—then you can unlock it without resetting the user password. This saves you from having to explicitly tell the user the new password. Instead, the user can simply log in by using the old password.

To unlock a user's account:

1. Search for the user account that you want to unlock by following the instructions described in "Searching for Entries by Using the Self-Service Console" on page 3-2.
2. Select the account that you want to unlock.
3. Choose **Unlock**. The Unlock User window appears.

   This window is described in "Unlock User" on page A-25.
4. The Unlock User window prompts you to confirm the unlocking of a user account. Click **Yes** to unlock the user account or **No** to return to the Users page.

**Note:** If a realm administrator's account becomes locked, the Oracle Internet Directory super user can unlock it by modifying the realm administrator's account password, using Oracle Directory Manager. See *Oracle Internet Directory Administrator's Guide* for information on how to use Oracle Directory Manager.

## Enabling User Accounts

If a user's account has been temporarily suspended—that is, disabled—then you can enable it. To do this:

1. Search for the user account that you want to enable by following the instructions described in "Searching for Entries by Using the Self-Service Console" on page 3-2.
2. Select the account that you want to enable.
3. Choose **Enable**. The Enable User window appears.

   This window is described in "Enable User" on page A-18.
4. The Enable User window prompts you to confirm the enabling of a user account. Click **Yes** to enable the user account or **No** to return to the Users page.

### Disabling User Accounts

You can temporarily suspend—that is, disable—a user's account. To do this:

1. Search for the user account that you want to disable by following the instructions described in "Searching for Entries by Using the Self-Service Console" on page 3-2.
2. Select the account that you want to disable.
3. Choose **Disable**. The Disable User window appears.

   This window is described in "Disable User" on page A-17.
4. The Disable User window prompts you to confirm the disabling of a user account. Click **Yes** to disable the user account or **No** to return to the Users page.

## Managing Resource Information

This section explains how to use the Self-Service Console to specify a new resource type and to configure default resource access information. It contains these topics:

- Specifying a New Resource Type
- Modifying Resource Types
- Deleting Resource Types
- Configuring Default Resource Access Information

### Specifying a New Resource Type

To specify a new resource type:

1. Select the **Configuration** tab, then choose **Preferences** to display the Preferences window.

   This window is described in "Preferences" on page A-23.
2. In the **Configure Resource Type Information** section, choose **Create**. The Create Resource Type window appears.

   This window is described in "Create Resource Type" on page A-15.
3. In the Create Resource Type window, enter values in the appropriate fields.
4. When you have entered all of the appropriate information in the Create Resource Type window, choose **Submit**. This returns you to the Preferences window. The resource type you just specified now appears under the **Resource Type Name** column.

> **See Also:** The section on resource information in the Concepts and Architecture chapter of the *Oracle Internet Directory Administrator's Guide* for a brief description of resource information

### Modifying Resource Types

To modify a resource type:

1. Select the **Configuration** tab, then choose **Preferences** to display the Preferences window.

   This window is described in "Preferences" on page A-23.
2. In the Preferences Window, select the resource whose information you want to modify from either the Configure Resource Type Information section or the

Default Resource Access Information section, and then choose **Edit**. The Edit Resource window appears.

This window is described in "Edit Resource" on page A-18.

3. In the Edit Resource window, modify the appropriate information.
4. Choose **Submit**.

## Deleting Resource Types

To modify a resource type:

1. Select the **Configuration** tab, then choose **Preferences** to display the Preferences window.

   This window is described in "Preferences" on page A-23.

2. In the Preferences Window, select the resource you want to delete from either the Configure Resource Type Information section or the Default Resource Access Information section, and then choose **Delete**. The Delete Resource window appears.

   This window is described in "Delete Resource" on page A-17.

3. Click **Yes** to delete the resource or **No** to return to the Preferences page.

## Configuring Default Resource Access Information

If you have a large number of users, then, instead of specifying resource access information for each user entry, you can define commonly used resources that all users automatically inherit. To do this:

1. Select the **Configuration** tab, then choose **Preferences** to display the Preferences window.

   This window is described in "Preferences" on page A-23.

2. In the **Default Resource Access Information** section, choose **Create**. The Create Resource window appears.

   This window is described in "Create Resource" on page A-15.

3. In the **Resource Name** field, specify the name of the resource or service to be accessed by the component on your behalf.
4. From the **Resource Type** list, select the type of resource to be accessed. Default options are:

   - **OracleDB**: Oracle Database 10*g*
   - **ExpressPDS**: Oracle Express Pluggable Data Source
   - **JDBCPDS**: Java Database Connectivity Pluggable Data Source

   Other resource types may appear in this list as specified by the administrator.

5. Choose **Next**. The Resource Access Information window appears.

   This window is described "Resource Access Information" on page A-24.

6. In the Resource Access Information window, enter the appropriate information into the fields.

7. Verify that you have entered all information correctly, then choose **Submit**. This returns you to the Preferences window. The default resource access information you just created now appears in the **Resource Name** column.

   **See Also:** The section on resource information in the Concepts and Architecture chapter of the *Oracle Internet Directory Administrator's Guide* for a brief description of resource information

# Part III

## Appendixes

Part III contains the following appendixes:

- Appendix A, "Elements in the Oracle Internet Directory Self-Service Console User Interface"
- Appendix B, "Troubleshooting Oracle Delegated Administration Services"

# A

# Elements in the Oracle Internet Directory Self-Service Console User Interface

This appendix lists and describes the various windows, fields, and control devices in the Oracle Internet Directory Self-Service Console.

## Windows and Fields in the Self-Service Console

This section lists and describes the windows and fields in the Self-Service Console. It contains these topics:

- Create Resource Type
- Create User
- Delete Category
- Delete Resource
- Delete User
- Disable User
- Edit Category
- Edit Group
- Edit My Profile
- Edit Resource
- Edit Service
- Edit Service Recipient
- Edit Subscription
- Edit User
- Editing Attribute
- Enable User
- General Provisioning
- Identity Management Realm Configuration
- Identity Management Realms
- Manage Defaults: Attributes
- Manage Defaults: Select Application
- Manage Group
- Manage Password
- Oracle Application Server Single Sign-On
- Order Category
- Organization Chart
- Preferences
- Provisioning Review
- Provisioning Search
- Reset My Single Sign-On Password
- Reset SSO Password
- Resource Access Information
- Search and Select
- Search for Groups
- Search for Users
- Services
- Session Level Diagnostic Settings

- Time Zone Settings
- Unlock User
- View Group
- View Identity Management Realm
- View My Profile
- View User

## Add/Edit Attribute

Use this window to add and edit attributes for user entries.

***Table A–1 Add/Edit Attribute Window***

| Field | Description |
|---|---|
| Directory Attribute Name | The attribute name (only available in the Add New Attribute window) |
| UI Label | Specify the friendly name of the attribute to be displayed in the user interface. For example, you can display the `sn` attribute as *Last Name* in the interface. |
| Required | Specify whether you want the attribute to be required in user creation and modification. Required attributes appear in the interface with an asterisk (*) to the left of the field. If you do not select this check box, then the attribute is optional. |
| Viewable | Specify whether you want the attribute to appear in search results by selecting this check box. |
| Self-Editable | Specify whether the end user can modify the value for this attribute in his or her own entry by using the Edit My Profile window. |
| Password Reset Validation | Specify one or more attributes that can be used to validate a user who forgets his or her password. |
| Searchable | By default, when a user enters a search request, the Oracle Internet Directory Self-Service Console searches based on the `cn`, `firstname`, `lastname`, and `e-mail` attributes. You can customize the attributes that can be searchable. For example, if you want to enable searching based on the attribute you are adding, then select this check box. The only restriction is that, to be searchable, the attribute must be cataloged. |

*Table A–1 (Cont.) Add/Edit Attribute Window*

| Field | Description |
|---|---|
| UI Type | Specify the type of interface for this field. Options are:<br>■ Single Line Text—a text field into which the user enters a value<br>■ Multi Line Text—a text area where a user can type multiple lines of text<br>■ Multi Line Single Value Text—a text area where a user can type multiple lines of text that is stored as a single value in Oracle Internet Directory<br>■ Predefined List--a combo box in which a user selects a value from a drop-down list. When you select this type of interface, the LOV Values text area appears. In that text area, enter the values for the list, pressing the ENTER key after each one.<br>■ Date—a text field into which the user enters a date—for example, an employee's birthday<br>■ Browse and Select User—a button enabling the user to browse for any user entry that needs a DN as an attribute value—for example, a manager entry<br>■ Browse and Select Group—a button enabling the user to browse for any group entry that needs a DN as an attribute value—for example, the default profile group<br>■ Number—a text field into which the user enters numbers only—for example, a postal code<br>■ Password—a text field into which the user enters a password value that is represented on screen using asterisks (*) for each letter. The Self-Service Console renders Password fields twice, with the second instance of the field assigned a label of Confirm Password.<br>■ Country List—a list of countries.<br>■ Language List—a list of languages.<br>■ Time Zone List—a list of time zones.<br>■ Check Box—a check box that specifies a value of true if checked or false if unchecked.<br>■ Date and Time—creates a text field into which the user enters a date along with three combo boxes from which the user selects hours, minutes, and the time zone |

**See Also:**

- "Configuring the Parent DN for Entries in a Realm" on page 5-3
- "Configuring User Entries" on page 5-5

## Advanced Search

Use this window to perform an advanced search for user entries.

*Table A–2 Advanced Search Window*

| Field | Description |
|---|---|
| Find users that match all conditions | Searches for users that match all conditions specified in this window |
| Find users that match any condition | Searches for users that match any of the conditions specified in this window |
| E-mail Address | Specifies an e-mail address to include in the search criteria |

*Table A–2 (Cont.) Advanced Search Window*

| Field | Description |
|---|---|
| First Name | Specifies a first name to include in the search criteria |
| Last Name | Specifies a last name to include in the search criteria |
| User Name | Specifies a user name to include in the search criteria |
| Add Another | Enables you to add additional attributes to the search criteria, including address, city, state, country, and manager |

**See Also:** Performing an Advanced Search on page 3-2

## All Object Classes

Use this window to add object classes for user entries.

**See Also:** "Configuring User Entries" on page 5-5

## Application Attributes

Use this window to set the various attributes available in each provisioned application for this user. You must enter information in all fields preceded by an asterisk (*).

Each provisioned application is listed as a separate drop-down display, which you can expand or hide by selecting the + or - buttons. Some provisioned applications may not have any attributes to set: these application lists will be empty even if you expand them.

*Table A–3 Oracle Calendar User Attributes*

| Component/Field | Default Value | Available Values | Description |
|---|---|---|---|
| Calendar Storage* | Based on policy | Default, or select from list of available storage, user entry | Which Calendar database to use for storing user's Calendar data |
| Calendar Access | TRUE | TRUE, FALSE | Use this option to turn on or off the user's access to Calendar. |
| Publish Status | Not Published | Not Published, Published | Determines whether this user's contact information is visible to other users. |
| Enable Global agenda view | TRUE | TRUE, FALSE | Determines whether this user's agenda information is visible to other users. |
| Alternate E-mail Address | null | user entry | Use this field to provide an alternate e-mail address. |
| Reminder Delivery Rule | Alternate | Alternate, Primary | The user can set two different appointment reminder preferences, and switch between them using this field. |
| Enable Alert | FALSE | TRUE, FALSE | Use this option to enable or disable Alerts. |
| Suspend Alert | FALSE | TRUE, FALSE | Temporarily disable alerts for a specified period. |

***Table A–3 (Cont.) Oracle Calendar User Attributes***

| Component/Field | Default Value | Available Values | Description |
|---|---|---|---|
| Suspend Alert period | 00:00-00:00 | Hours:minutes-Hours:minutes | Specify duration for alerts to be suspended. |
| Alert Suspension Period Action | Send Alerts | Discard Alerts, Hold Alerts, Send Alerts | During alert suspension period, option determines what should happen to incoming alerts. |
| Send Alert on Meeting | TRUE | TRUE, FALSE | Default behavior for this user to receive or not receive alerts when a meeting is created or modified. Meeting owner can override this setting. |
| Send Alert on Day Event | FALSE | TRUE, FALSE | Default behavior for this user to receive or not receive alerts when a day event is created or modified. Event owner can override this setting. |
| Send Alert on Daily Note | FALSE | TRUE, FALSE | Default behavior for this user to receive or not receive alerts when a Daily Note is created or modified. Note owner can override this setting. |
| Send Alert on Journal | FALSE | TRUE, FALSE | Default behavior for this user to receive or not receive alerts when a journal entry is created or modified. Journal owner can override this setting. |
| Send Alert on Owned Event | TRUE | TRUE, FALSE | Default behavior for this user to receive or not receive alerts when an event owned by this user is created or modified. |
| Send Alert on Declined Event | FALSE | TRUE, FALSE | Default behavior for this user to receive or not receive alerts when an event the user has declined is modified. Event owner can override this setting |

***Table A–4 Oracle Mail User Attributes***

| Component/Field | Default Value | Available Values | Description |
|---|---|---|---|
| E-mail Quota (M)* | null | Numbers (Megabytes) | Size of user's allocated storage on the server. |
| Information Store | null | Default, <list of available>? | If there are multiple Information storage units, select one for this user. |
| User Status | Active | Active, Inactive | An Active user is a user with all permissions to access. An Inactive user cannot access the mail system at all. However, messages sent to an Inactive account are stored in the information store and can be accessed once the account is activated. |
| Auto Reply Mode | null | Echo, Reject, Reply, Vacation | Users can modify their reply mode. Echo replies with a copy of the sender's message along with the Auto Reply Text. Reject rejects all incoming messages. Reply replies to every incoming message with the Auto Reply Text only. Vacation replies with only one message for each sender, with the Reply Text. |
| Auto Reply Text | null | user entry | If the Auto Reply Mode is set to Reply, this text will be included in the Reply message. |
| Auto Reply Expiration | null | mm/dd/yyyy | This date sets when Auto Reply Mode will switch back to normal delivery mode. |
| Forward E-mail Address | null | user entry | When Auto-Reply is on, all messages will be forwarded to this address. If this attribute is blank, messages will not be forwarded. |

***Table A–4 (Cont.) Oracle Mail User Attributes***

| Component/Field | Default Value | Available Values | Description |
|---|---|---|---|
| Text Indexing | none | Disable, Enable | When Text Indexing is enabled, Oracle Collaboration Suite 10*g* Search can access message body content and header information. When it is disabled, messages are not indexed and no search can be performed. |
| Role | User | Domain Administrator, System Administrator, User | Specifies the permissions for this user: A domain administrator will have permissions to administer and configure Oracle Mail within a particular domain; A system administrator will have permissions to administer and configure the entire Oracle Mail system; A user will only have permissions to access, read, and send messages. |
| Archive Policy | null | Default, <list of available>? | Select an archiving policy to assign to the user. Using the e-mail archive feature, an administrator can assign a message archiving policy for each user. Each policy will create a copy of all mail messages to and from that user, including envelope information for those messages, and forward those copies to an e-mail address specified in Oracle WebMail administration. The specified e-mail address may then be used by an archiving tool to create an archive. |

***Table A–5 Oracle Voicemail & Fax User Attributes***

| Component/Field | Default Value | Available Values | Description |
|---|---|---|---|
| International Phone Number* | null | user entry | Specify the unique phone number for this voice mail user. |
| Group Name* | null | list of available groups | You can assign the user to any available group. |
| Voicemail Password* | null | user entry | Create or reset the user's password. |
| Confirm Password* | null | user entry | Enter the password again in this box. The password must match the Voicemail Password exactly. |

*Table A–5 (Cont.) Oracle Voicemail & Fax User Attributes*

| Component/Field | Default Value | Available Values | Description |
|---|---|---|---|
| Voice Preferred Language | null | American English, Arabic, Brazilian Portuguese, British English, Danish, Dutch, Finnish, French, German, Greek, Italian, Japanese, Korean, Mandarin-China, Mandarin-Taiwan, Norwegian, Portuguese, Spanish, Swedish, Turkish | Select an available language to be used for this voice mail user's voice prompts. |
| Phone Access Allowed | null | true, false, Group Default | You can set the user to have access to voice mail, deny access, or inherit the permission setting from the user's group. |
| Faxin Access Allowed | null | true, false, Group Default | You can set the user to have access to Faxin functions, deny access, or inherit the permission setting from the user's group. |
| Message Waiting Indicator | null | true, false, Group Default | If the user's phone has a message waiting indicator, enabling this option allows it to be used by the system to indicate whenever the user has new voice mail messages. Group Default causes the user to inherit the permission setting from the user's group. |
| Additional Voice Quota | null | Numbers (bytes) | Voicemail is stored in the user's E-mail Quota, but you can allocate additional storage space to be used only for voice mail. This can help prevent large voice mail messages from filling up the user's Email quota. |

**See Also:** The chapter on managing with the Oracle Provisioning Console in the *Oracle Identity Management Integration Guide*

## Application Provisioning

Use this window to view the default provisioning policies for each deployed component of Oracle Collaboration Suite. If the default policy allows, you can override the policy by choosing to Provision or Do Not Provision any component. If the default policy does not allow you to override it, then the Override Policy section will be grayed out.

Each component is listed along with its default policy (Required is set to Yes or No), and Override Policy buttons (Provision or Do Not Provision).

**See Also:** The chapter on managing with the Oracle Provisioning Console in the *Oracle Identity Management Integration Guide*

## Application-Level Diagnostic Settings

Use this window to view and configure application level diagnostic settings.

**See Also:** "Viewing and Configuring Application Diagnostic and Logging Settings" on page B-4

## Assign Privileges to Group

Use this window to specify access rights for a group entry.

***Table A–6 Assign Privileges to Group Window***

| Privilege | Description of Access Granted |
|---|---|
| Allow user creation | Create user entries |
| Allow user editing | Modify user entries |
| Allow user deletion | Delete user entries |
| Allow group creation | Create group entries |
| Allow group editing | Modify group entries |
| Allow group deletion | Delete group entries |
| Allow privilege assignment to users | Assign access rights to users |
| Allow privilege assignment to groups | Assign access rights to groups |
| Allow service management | Enable group members to manage services for users. If this is selected, then a **Services** link becomes available in the **Directory** tab page when the latter is accessed by group members. |
| Allow account management | Enable group members to manage accounts for users. If this is selected, then a group member can enable, disable, and unlock users in the Search for Users results page. |
| Allow Oracle Delegated Administration Services configuration | Configure Oracle Delegated Administration Services user interface |
| Allow User Management and Application Provisioning | Create, edit, delete, and assign privileges to users |

**See Also:** "Assigning Privileges to Groups" on page 5-12

## Assign Privileges to User

Use this window to specify access rights for a user entry.

***Table A–7 Assign Privileges to User Window***

| Privilege | Description of Access Granted |
|---|---|
| Allow account management | Enable, disable, and unlock user accounts |
| Allow group creation | Create group entries |

*Table A–7 (Cont.) Assign Privileges to User Window*

| Privilege | Description of Access Granted |
|---|---|
| Allow group deletion | Delete group entries |
| Allow group editing | Modify group entries |
| Allow Oracle Delegated Administration Services configuration | Configure Oracle Delegated Administration Services user interface |
| Allow privilege assignment to groups | Assign access rights to groups |
| Allow privilege assignment to users | Assign access rights to users |
| Allow resource management for Oracle Reports- and Forms-based applications | Configure resources such as databases or applications |
| Allow service management | Manage services for users. If this is selected, then a **Services** link becomes available in the **Directory** tab page when the latter is accessed by group members. |
| Allow user creation | Create user entries |
| Allow user deletion | Delete user entries |
| Allow user editing | Modify user entries |
| Allow User Management and Application Provisioning | Create, edit, delete, and assign privileges to users—only available if the currently logged in user has also been assigned this privilege |

**See Also:** "Assigning Privileges to Users" on page 5-10

## Bulk User Management

Use this window to create, edit, or delete users in bulk mode by specifying an LDIF (LDAP Data Interchange Format) file containing user data. If you select the Ignore Failed Users box, the bulk create process will attempt to create, edit, or delete users regardless of failures. Failed users will be placed in a file you can download at the end of the process. If you do not select the Ignore Failed Users box, the bulk management process will terminate at the first failed user.

**See Also:** "Managing Users in Bulk" on page 5-9

## Change Application Password

Use this window to change the password of the Oracle component you previously selected in the Manage My Password window. The new password you specify must conform to any relevant password policy set by the administrator. Enter the new password for the component, and then confirm it. You can erase what you have entered in these fields by choosing **Clear**. When you finish entering the values, choose Submit.

**See Also:** "Changing Your Own Password and Password Hint" on page 4-2

## Configure Attribute Categories

Use this window to customize the way that categories of attributes are displayed to a user who is adding or modifying an entry. Specifically, you can use this window to customize the name of each category and the order in which it is displayed.

**See Also:** "Configuring User Entries" on page 5-5

## Configure Roles

Use this window to specify the roles that users can assign to others.

**See Also:** "Configuring User Entries" on page 5-5

## Configure Search Table Columns

Use this window to specify the attributes that display in a search table. You can use the Move, Move All, Remove, and Remove All buttons to move attributes between the All Attributes and the Selected Attributes lists. You can also use the buttons to the right of the Selected Attributes list to move attributes up or down in the list.

**See Also:** "Configuring User Entries" on page 5-5

## Configure User Attributes

Use this window to view, add, modify, and delete attributes for user entries. See "Add/Edit Attribute" on page A-3 for a listing of the available fields in this window.

**See Also:**

- "Configuring the Parent DN for Entries in a Realm" on page 5-3
- "Configuring User Entries" on page 5-5

## Configure User Object Classes

When you create user entries, use this window to view and add the object classes.

This window displays the object classes commonly associated with user entries. To add other object classes to a user entry, choose Add Object Class.

**See Also:**

- "Configuring the Parent DN for Entries in a Realm" on page 5-3
- "Configuring User Entries" on page 5-5

## Confirm Additional Personal Information

If you forget and want to reset your password, then use this window to provide information that the server can use to validate your identity.

If you set your password hint, then this window asks you a question based on that hint. Enter the answer to the password hint you specified.

If you did not previously set a password hint, then this window prompts you for other personal data as configured by your administrator.

**See Also:** "Resetting Your Password If You Forget It" on page 4-2

## Confirmation of Deletion

This window displays information about the group and prompts you to confirm deletion.

**See Also:** "Deleting Group Entries" on page 5-12

## Create Category

When creating a new attribute category, use this window to specify the UI Label—that is, the name of the category as it is displayed to the user.

**See Also:** "Configuring User Entries" on page 5-5

## Create Group

Use this window to create a group entry. You must enter information in all fields preceded by an asterisk (*). Table A–8 lists the fields in this window.

***Table A–8 Create Group Window***

| Field | Description |
|---|---|
| **Basic Information** | |
| Name | Enter a name for this group. This will be used as the RDN for this group. |
| Display Name | Enter a friendly name for this group. For example, if the RDN is `OracleDBCreators`, then you could enter the display name as `Oracle Database Creators`. |
| Description | (Optional) Enter a brief description of this group. |
| Group Visibility | To hide this group from all but its owners, select Private. Otherwise, accept the default, Public. |
| Make this group privileged. | Select this box if you want to assign privileges to this group. You cannot assign privileges to a non-privileged group. |
| **Owners** | Use this section to add or remove owners of this group.<br>To add a user as an owner of this group:<br>1. In the Owners section, choose Add User. This displays the Search and Select: User window.<br>2. Search for the entry of the user you want to add as an owner of the group.<br>3. Choose Select. This returns you to the Create Group window. The user you specified is listed in the Owners section.<br>To add a group as an owner of this group:<br>1. In the Owners section, choose Add Group. This displays the Search and Select: Group window.<br>2. Search for the entry of the group you want to add as an owner of the group.<br>3. Choose Select. This returns you to the Create Group window. The group you specified is listed in the Owners section.<br>To remove a user or group as an owner of this group, select the user or group, then choose Remove. |

*Table A–8 (Cont.) Create Group Window*

| Field | Description |
|---|---|
| **Members** | Use this section to configure members of this group.<br>To add a user as a member of this group:<br>1. In the **Members** section, choose **Add User**. This displays the Search and Select window.<br>2. Search for the entry of the user you want to specify as a member of this group.<br>3. Choose **Select**. This returns you to the Create Group window. The user you specified is listed in the **Members** section.<br>To remove a user from this group, in the **Members** section, select the user's name and choose **Remove**.<br>To add a group as a member of this group:<br>1. In the **Members** section, choose **Add Group**. This displays the Search and Select window.<br>2. Perform a search for the entry of the group you want to specify as a member of this group, then choose **Select**. This returns you to the Create Group window. The group you specified is listed in the **Members** section. |
| **Roles Assignment** | Use this section to assign roles to this group.<br>To specify the roles that you want to assign to this group, in the **Roles Assignment** section, in the **Select** column, select the role that you want to assign to this group.<br>To remove the role from the group, in the **Roles Assignment** section, in the **Select** column, deselect the role that you want to remove from this group. |

**See Also:** "Creating Group Entries" on page 5-12

## Create Identity Management Realm

As the administrator for a service provider, you can use this window to create a new Identity Management Realm entry that includes the following information:

- The name of the realm and that of the contact person for it
- The display of realm and product logos

*Table A–9 Create Identity Management Realm Window*

| Field | Description |
|---|---|
| **Basic Information** | |
| Realm Name | Enter a relatively short version of the name of the realm for this realm. The name you enter is used to create the DN for this realm entry. This field is mandatory. |
| Realm Contact | Enter the name of the person to contact for any issues regarding this realm. |
| Description | Enter any additional information about this realm. This field is optional. |
| **Logo Management** | |
| Enable Realm Logo | Select to display the realm logo on the Identity Management Realm Configuration window. |

*Table A–9 (Cont.) Create Identity Management Realm Window*

| Field | Description |
|---|---|
| Enable Product Logo | Select to display the product logo on the Identity Management Realm Configuration window.<br><br>**Note:** If both Enable Realm Logo and Enable Product Logo are selected, then the realm logo appears at the top, with the product logo beneath it. |
| Update Realm Logo | Enter the path and file name of the logo for this realm or, alternatively, navigate to it by choosing **Browse**. |

**See Also:** "Creating an Additional Identity Management Realm" on page 5-4

## Create Resource

Use this window to specify a name and type when creating a new resource.

**See Also:** "Creating Resource Access Information" on page 4-4

## Create Resource Type

If you have the correct privileges, then you can use the Create Resource Type window to create a resource type.

*Table A–10 Create Resource Type Window*

| Property | Description |
|---|---|
| Resource Type Name | Name that describes the type of resource. |
| Display Name | Name to be used when the resource type appears in the user interface. |
| Description | Textual description that explains the purpose of the resource type and any other information you want to enter for it. |
| Authentication Class | Leave this field blank. |

*Table A–10 (Cont.) Create Resource Type Window*

| Property | Description |
|---|---|
| Connection String | Format for constructing the connection string using the values stored in Oracle Internet Directory for the resource. For example:<br>■ For the Oracle9*i* Database Server or a JDBC data source your connection string format might be:<br>`orclUserIDAttribute/orclPasswordAttribute @orclFlexAttribute1`<br>This string indicates that the user name is followed by a slash, the password, an at sign (@), and then additional attribute 1—for example, for the TNS name of the database. A connection string that adheres to this format would look similar to this one:<br>`scott/tiger@db1`<br>■ For Oracle Express your connection string format might be: server=orclFlexAttribute1/domain=orclFlexAttribute2/user= orclUserIDAttribute/password=orclPasswordAttribute<br>This string indicates that server= is followed by the first additional attribute, a slash, domain=, the second additional attribute, a slash, the user name, a slash, and the password. A connection string that adheres to this format would look similar to this one:<br>`server=a1/domain=a2/user=scott/password=tiger` |
| User Name/ID Field Name | Display name of the user name field that appears on the Create Resource window when a user creates new resource access information. Typically, this display name is something like "Username" or "User Name". |
| Password Field Name | Display name of the password field in the Create Resource window. Typically, this display name is "Password". |
| Additional Fields | Display name of the additional fields displayed in the Create Resource window beyond user name and password. For example, you might use one of these fields to contain a server or domain name. Typically, this display name is descriptive of the field contents, such as "Server" or "Domain". |

**See Also:**

- "Managing Your Own Resource Information" on page 4-4
- "Specifying a New Resource Type" on page 5-16
- "Configuring Default Resource Access Information" on page 5-17

## Create User

Use this window to create a user entry by providing appropriate information in the various fields. You must enter information in all fields preceded by an asterisk (*).

In this window, some of the sections are unique to your environment, others are integral to the Self-Service Console. The latter are:

- **Roles Assignment**, which enables you to assign one or more roles to this user
- **Resource Access Information**, which enables you to grant this user access to resources specific to Oracle Forms and Oracle Reports.

Enter values in the fields unique to your environment.

**Note:** You cannot use a tilde (~) in a user ID.

**See Also:** "Creating User Entries" on page 5-8

## Delete Category

This window prompts you to confirm deletion of an attribute category.

**See Also:** "Configuring User Entries" on page 5-5

## Delete Resource

This window displays information about the resource and prompts you to confirm deletion.

**See Also:**

- "Deleting Resource Access Information" on page 4-5
- "Deleting Resource Types" on page 5-17

## Delete User

This window displays information about the user and prompts you to confirm deletion.

**See Also:** "Deleting User Entries" on page 5-9

## Disable User

This window prompts you to confirm the disabling of a user account.

**See Also:** "Disabling User Accounts" on page 5-16

## Edit Category

Use this window to edit an attribute category. You can use the Move, Move All, Remove, and Remove All buttons to move attributes between the Unused Attributes and the Selected Attributes lists. You can also use the buttons to the right of the Selected Attributes list to move attributes up or down in the list.

**See Also:** "Configuring User Entries" on page 5-5

## Edit Group

Use this window to edit a group entry. You must enter information in all fields preceded by an asterisk (*).

**See Also:** "Modifying Group Entries" on page 5-12

## Edit My Profile

Use this window to change the information in your profile. You must enter a value in any field marked with an asterisk (*).

**See Also:** "Editing Your Profile" on page 4-4

## Edit Resource

Use this window to modify resource access information.

**See Also:**

- "Modifying Resource Access Information" on page 4-5
- "Modifying Resource Types" on page 5-16

## Edit Service

Use this window to change the display name and network address for a service.

**See Also:** "Managing Services" on page 5-13

## Edit Service Recipient

Use this window to edit a subscription list for a service recipient.

**See Also:** "Modifying Subscription Information for a Service Recipient" on page 5-14

## Edit Subscription

From this window, you can add, modify, or delete the subscription list for a service recipient.

**See Also:** "Managing Services" on page 5-13

## Edit User

Use this window to:

- Modify values in a user entry
- Specify resource access information for a user
- See a list of groups that this user is a member of

**See Also:** "Modifying User Entries" on page 5-8

## Editing Attribute

Use this window to find and modify information about a user entry. See "Add/Edit Attribute" on page A-3 for a listing of the available fields in this window.

**See Also:** "Configuring User Entries" on page 5-5

## Enable User

This window prompts you to confirm the enabling of a user account.

**See Also:** Enabling User Accounts on page 5-15

## General Provisioning

Use this window to enter general provisioning information for a user entry. You must enter information in all fields preceded by an asterisk (*).

***Table A–11 General Provisioning Window***

| Field | Description |
|---|---|
| **Basic Information** | |
| First Name | Specifies a user's first name |
| Middle Name | Specifies the user's middle name |
| Last Name | Specifies a user's last name |
| User Name | Specifies a user name |
| Password | Sets an initial password |
| Confirm Password | Confirms the initial password |
| Email Address | Specifies a user's e-mail address |
| Time Zone | Specifies the user's time zone |
| User Default Group | Identifies the user's default group |
| **Additional Personal Details** | |
| Is Enabled | Determines whether the user entry is enabled |
| Start Date | Specifies the user's start date |
| End Date | Specifies the user's end date |
| Known As | Specifies an alias the user is known as |
| Maiden Name | Specifies the user's maiden name |
| Date of Birth | Specifies the user's date of birth |
| Language | Specifies the user's default language |
| **Organizational Details** | |
| Employee Number | Specifies the user's employee number |
| Job Title | Specifies the user's job title |
| Department | Identifies the user's department |
| Manager | Identifies the user's manager |
| Assistant | Identifies the user's assistant |
| Hire Date | Specifies the user's hire date |
| **Photograph** | Enables you to upload a user's photograph |
| **Telephone Numbers** | |
| Work Phone | Contains the user's work phone |
| Home Phone | Contains the user's home phone |
| Mobile Phone | Contains the user's mobile phone |
| Pager | Contains the user's pager number |
| Fax | Contains the user's fax number |
| **Office Address** | |
| Address | Identifies the user's office address |
| City | Identifies the user's city |
| State | Identifies the user's state |

*Table A–11 (Cont.) General Provisioning Window*

| Field | Description |
|---|---|
| ZIP Code | Identifies the user's zip code |
| Country | Identifies the user's country |
| **Home Address** | Identifies the user's home address |
| **Role Assignment** | Enables you to assign one or more roles to this user |
| **Resource Access Information** | Enables you to grant this user access to resources specific to Oracle Forms and Oracle Reports. |

**See Also:** The chapter on managing with the Oracle Provisioning Console in the *Oracle Identity Management Integration Guide*

## Identity Management Realm Configuration

Use this window to configure the entry for an identity management realm.

*Table A–12 Identity Management Realm Window*

| Field | Description |
|---|---|
| **Directory Configuration** | |
| Attribute for Login Name | Enter the attribute by which you want users to identify themselves when they log in--for example, `UID`, `EmployeeNumber`, `SSN`.<br>This is the attribute that uniquely identifies the user. Oracle Application Server Single Sign-On locates the user by using this attribute during login. When you make changes to this attribute, be sure that the user entries contain this attribute and are unique. You can enforce the uniqueness by setting up an attribute uniqueness constraint on this attribute under the user search base.<br>This field is mandatory. |
| Attribute for RDN | The attribute used for creating the RDN component of the user entry. The value you enter for this field should not be the same as the value you entered in the Attribute for Login Name field. |
| User Search Base | Enter the DN of the entry under which the user entries for this realm are located.Make sure you enter the valid DN and users are present under this context. Oracle Application Server Single Sign-On looks for users under this context during user login.<br>Also, be sure that all the ACLs are set up properly. Any discrepancy among the ACLs will disrupt either the login process or the behavior of Oracle Internet Directory Self-Service Console.<br>This field is mandatory. |

*Table A–12 (Cont.) Identity Management Realm Window*

| Field | Description |
|---|---|
| User Creation Base | Enter the DN of the entry under which to create users for this realm. This should be the same as that for the user search base.<br>If you want to distribute the users under different contexts under the user search base, then you can set this value to be different than that of the user search base. In either case, this DN should be either that of the user search base, or of a context under the user search base. For example, if the user search base is `cn=users,dc=acme,dc=com`, and you want to divide the users based on the locality, then you can set this value to:<br>`L=America, cn=users,dc=acme,dc=com`<br>`L=Asia, cn=users,dc=acme,dc=com`<br>`L=Europe, cn=users,dc=acme,dc=com`<br>**Note:** The Oracle Internet Directory Self-Service Console expects these contexts to be present and the privileges under these contexts to be set correctly. |
| Group Search Base | Enter the DN of the entry under which group entries for this realm are located. This field is mandatory. |
| Group Creation Base | Enter the DN of the entry under which to create groups for this realm |
| Search Return Limit | Enter the maximum number to be displayed in a search. This field is mandatory. |
| **Logo Management** | |
| Enable Realm Logo | Select to display the realm logo on the Identity Management Realm Configuration window. |
| Enable Product Logo | Select to display the product logo on the Identity Management Realm Configuration window.<br>**Note:** If both Enable Realm Logo and Enable Product Logo are selected, then the realm logo appears at the top, with the product logo beneath it. |
| Update Realm Logo | Enter the path and file name of the logo for this realm or, alternatively, navigate to it by choosing **Browse**. |

**See Also:** "Configuring an Identity Management Realm" on page 5-2

## Identity Management Realms

If you have the administrative privileges, then you can use this window to create or view a subscriber entry.

## Manage Defaults: Attributes

This window displays all user attribute fields for each application you selected in the Manage Defaults: Select Application window. You can set the default attribute for each displayed field. The default settings will appear in the Application Attributes window any time a new user is created. Changing defaults will not affect existing users, even if those users were created using previous default values. For complete descriptions of the fields in this window, see "Application Attributes" on page A-5.

**See Also:** The chapter on managing with the Oracle Provisioning Console in the *Oracle Identity Management Integration Guide*

## Manage Defaults: Select Application

Use this window to select the applications for which you want to manage defaults. The available applications listed in this window will vary according to your environment.

**See Also:** The chapter on managing with the Oracle Provisioning Console in the *Oracle Identity Management Integration Guide*

## Manage Group

If you have the necessary privileges, then you can use this window to edit the information in a group entry or to delete a group. The appropriate buttons appear depending on your privileges.

**See Also:** "Modifying Group Entries" on page 5-12

## Manage Password

This window enables you to change your passwords for OracleAS Single Sign-On and various Oracle components. Note that the new password you specify must conform to any relevant password policy set by the administrator.

**See Also:** "Changing Your Own Password and Password Hint" on page 4-2

## Oracle Application Server Single Sign-On

This window appears if your deployment of the Self-Service Console is enabled for OracleAS Single Sign-On. Use it to enter your OracleAS Single Sign-On user name and password.

## Order Category

Use the window to reorder your category list. When a user creates or edits her entry, the interface displays various categories—for example, one category might simply be "Basic Information," and another might be "Telephone Numbers." Each category prompts the user for values for various attributes. For example, the "Basic Information" category could prompt for first and last names, home address, zip code, and department; the "Telephone Numbers" category could prompt for home phone, work phone, mobile phone, and fax. You can use the buttons to the right of the Category List to move categories up or down in the list.

**See Also:** "Configuring User Entries" on page 5-5

## Organization Chart

Use this window to locate yourself within the hierarchy of your organization. To see the entries under a name, choose the plus sign (+) next to that name. To see details for a given entry, choose the entry.

**See Also:** "Viewing Your Organizational Chart" on page 4-4

## Preferences

Use this window to create, edit, and delete resource types and to configure default resource access information.

**See Also:** "Managing Resource Information" on page 5-16

## Provisioning Review

Use this window to review provisioning information before creating or modifying a user entry.

**See Also:** The chapter on managing with the Oracle Provisioning Console in the *Oracle Identity Management Integration Guide*

## Provisioning Search

Use this window to search for users based on their provisioning status in a provisioning-enabled application. The provisioning-enabled applications that are listed in this window will vary according to your environment.

***Table A–13 Provisioning Search Window***

| Field | Description |
|---|---|
| Find users that match all conditions | Searches for users that match all conditions specified in this window |
| Find users that match any condition | Searches for users that match any of the conditions specified in this window |
| Provisioning Status for application | Searches for the user's provisioning status in this application; a separate Provisioning Status field will appear in this window for each provisioning-enabled application that is installed in your environment |
| Add Another | Enables you to add additional attributes to the search criteria, including address, city, state, country, and manager |

**See Also:** The chapter on managing with the Oracle Provisioning Console in the *Oracle Identity Management Integration Guide*

## Reset My Single Sign-On Password

If you forget your password, then you can reset it by first filling in the fields on this page. This information is used to identify you to the server.

**See Also:** "Resetting Your Password If You Forget It" on page 4-2

## Reset SSO Password

If you forget and want to reset your password, then use this window to enter a new password and then confirm it.

**See Also:** "Resetting Your Password If You Forget It" on page 4-2

## Resource Access Information

Use this window to specify resource access information for a user. More specifically, use it to specify the username and password and the name of the database that you want the user to access.

**See Also:** "Configuring Default Resource Access Information" on page 5-17

## Search and Select

Use this window to search for users and add them to a subscription list.

**See Also:** "Managing Services" on page 5-13

## Search for Groups

Use this window to search for group entries in the directory. If you have the appropriate privileges, then you can also create group entries.

**See Also:** "Searching for Group Entries by Using the Self-Service Console" on page 3-2

## Search for Users

Use this window to search for user entries in the directory. If you have the appropriate privileges, you can also use it to create user entries.

**See Also:** Searching for User Entries by Using the Self-Service Console on page 3-2

## Services

This window lists the various services available in your domain. You can choose the appropriate button to:

- Edit Services—that is, change the display name and network for each service
- Edit Subscriptions—that is, specify service recipients, the users on their respective subscription lists, and the timeframe within which those users can access the services.

**See Also:** "Managing Services" on page 5-13

## Session Level Diagnostic Settings

Use this window to view and configure session level diagnostic settings.

**See Also:** "Viewing and Configuring Session-Level Diagnostic Settings" on page B-4

## Time Zone Settings

Use this window to change the setting for your time zone.

**See Also:** "Changing Your Time Zone Setting" on page 4-3

## Unlock User

This window prompts you to confirm the unlocking of a user account.

**See Also:** Unlocking User Accounts on page 5-15

## View Group

This window displays information for the selected group.

**See Also:** "Viewing Group Entries" on page 5-11

## View Identity Management Realm

This window displays information for the selected realm.

**See Also:** "Viewing Configuration Settings for Additional Identity Management Realms" on page 5-4

## View My Profile

This window displays the latest information you provided about yourself. To change this information, choose **Edit My Profile**.

---

**Note:** To refresh this window with the latest information in the server, choose Refresh My Profile. Do not use the refresh or reload button on your browser, which simply refreshes with information from the mid-tier cache and not from the server.

---

**See Also:** "Viewing Your Profile" on page 4-1

## View User

This window displays profile information for the selected user.

**See Also:** "Viewing User Entries" on page 5-8

# B

# Troubleshooting Oracle Delegated Administration Services

This appendix describes common problems that you might encounter when using Oracle Delegated Administration Services and explains how to solve them. It contains these topics:

- Analyzing Log Files
- Enabling Debugging
- Diagnosing Self-Service Console Problems
- Diagnosing Service Unit Problems
- Need More Help?

> **Note:** You can also use Web browser diagnostics to identify basic problems with your Oracle Delegated Administration Services deployment, including whether the IP address and host name are valid or if a firewall is properly forwarding requests and responses. For more information, see the documentation for the Web browsers you plan to support in your Oracle Delegated Administration Services deployment.

## Analyzing Log Files

If you encounter problems when deploying or running Oracle Delegated Administration Services, you should first examine the various log files that are generated by Oracle Delegated Administration Services and the various components that it requires. This section contains the following topics:

- Oracle Delegated Administration Services Logs
- Oracle Containers for J2EE Logs
- Oracle HTTP Server Logs
- OPMN Logs

### Oracle Delegated Administration Services Logs

Oracle Delegated Administration Services logs most errors in the following log file:

`$ORACLE_HOME/opmn/logs/OC4J~OC4J_SECURITY~default_island~1`

This is the file you should check first when troubleshooting problems with Oracle Delegated Administration Services. Debugging must be enabled before Oracle Delegated Administration Services writes any information to the log file. To enable debugging, follow the instructions in "Enabling Debugging" on page B-3.

> **See Also:** "Viewing and Configuring Session-Level Diagnostic Settings" on page B-4 for information on how to view and configure diagnostic settings for Oracle Delegated Administration Services

## Oracle Containers for J2EE Logs

Oracle Containers for J2EE is the servlet engine that receives Oracle Delegated Administration Services page requests. You can examine the servlet access log, named default-web-access.log, in the $*ORACLE_HOME*/j2ee/OC4J_SECURITY/log/OC4J_SECURITY_default_island_1 directory. You can also examine the application.log file, which contains run-time application errors, in the $*ORACLE_HOME*/j2ee/OC4J_SECURITY/application-deployments/oiddas/OC4J_SECURITY_default_island_1 directory.

## Oracle HTTP Server Logs

Oracle HTTP Server receives requests for Oracle Delegated Administration Services pages and forwards each request to the appropriate component for further processing. For problems that may be related to Oracle HTTP Server, you can examine the log files located in the $*ORACLE_HOME*/Apache/Apache/logs directory. Specifically, you should examine the access_log and error_log files.

> **Note:** If Oracle HTTP Server is configured to rotate its log files, it appends a timestamp extension to the `access_log` and `error_log` files. Use the timestamp extension to find the most recent files.

## OPMN Logs

Errors that occur when Oracle Delegated Administration Services first starts are recorded in the $*ORACLE_HOME*/opmn/logs/OC4J~OC4J_SECURITY~default_island~1 file, which is generated by Oracle Containers for J2EE. Check this file for error messages if the `opmnctl` utility hangs or generates command-line errors when attempting to start Oracle Delegated Administration Services.

The $*ORACLE_HOME*/opmn/logs/ipm.log file also contains basic information regarding the OC4J_SECURITY process, which can be helpful in determining the overall health of your Oracle Delegated Administration Services implementation. Search the ipm.log file for "OC4J_SECURITY" and review any errors you find. The log file typically contains the following messages for OC4J_SECURITY:

```
Starting Process: OC4J~OC4J_SECURITY~default_island~1
Process Alive: OC4J~OC4J_SECURITY~default_island~1
Stopping Process: OC4J~OC4J_SECURITY~default_island~1
Process Stopped: OC4J~OC4J_SECURITY~default_island~1
Restarting Process: OC4J~OC4J_SECURITY~default_island~1
```

The ipm.log file also contains messages describing any problems that may have occurred with the OC4J_SECURITY process. For example, the log file will contain the following message if OPMN encounters any problems while starting the OC4J_SECURITY process:

```
Infra.us.oracle.com~OC4J~OC4J_SECURITY~default_island~1952317603:0
  Status: NONE
  Operation: internal (oid dependency failed)
  ErrFile:
  String: OID
```

## Enabling Debugging

To enable or disable debugging for Oracle Delegated Administration Services, you modify the DEBUG and DEBUG_LEVEL flags in the $*ORACLE_HOME*/ldap/das/das.properties file. Table B–1 describes each flag.

***Table B–1 Debugging Flags in the das.properties File***

| Flag | Description | Values | Default Value |
|---|---|---|---|
| DEBUG | Determines whether debugging is enabled | true<br>false | false |
| DEBUG_LEVEL | Specifies the debugging level | error (logs all errors)<br>schema (logs errors related to Oracle Internet Directory schema operations)<br>tracing (logs detailed tracing information for various operations)<br>session (logs information on operations involving the Oracle Delegated Administration Services connection pool or connection retrieval and release) | none |

The DEBUG_LEVEL flag is only interpreted if the DEBUG flag is assigned a value of true. Separate the value assigned to each flag with a vertical bar (|). For example, the following statements assign a value of true to the DEBUG flag and a value of tracing to the DEBUG_LEVEL flag:

```
DEBUG|true
DEBUG_LEVEL|tracing
```

After modifying the das.properties file, you must restart the Oracle Delegated Administration Services instance. Before restarting Oracle Delegated Administration Services, you may want to consider deleting the existing ipm.log file in order to create a fresh log file that does not contain any messages from previous Oracle Delegated Administration Services instances.

> **See Also:** "Starting and Stopping Oracle Delegated Administration Services" on page 1-7

## Diagnosing Self-Service Console Problems

This section describes how to troubleshoot problems with the Self-Service Console. It contains these topics:

- Viewing and Configuring Application Diagnostic and Logging Settings
- Viewing and Configuring Session-Level Diagnostic Settings
- Setting Unit-Level Diagnostic Settings

- Diagnosing Login Problems
- Users Prompted to Change Password Multiple Times
- Missing User Entries
- Interpreting Error Messages
- Handling with Pop-Up Window Blocking
- Handling Cross-Domain Invocation Issues
- Troubleshooting SSO Login Issues

You can use the diagnostic settings in Oracle Delegated Administration Services to debug your implementation without having to examine the log files. If you have configuration privileges, then you can also change the runtime logging levels without restarting Oracle Delegated Administration Services.

**See Also:** Appendix B, "Troubleshooting Oracle Delegated Administration Services"

## Viewing and Configuring Application Diagnostic and Logging Settings

You can view and configure application level diagnostic settings for all user sessions and all units in an Oracle Delegated Administration Services application. Diagnostic settings can be turned on or off. If an application-level diagnostic setting is turned on, diagnostics will display, unless overridden by session-level or unit-level diagnostic settings. If an application-level diagnostic setting is turned off, diagnostics will not display, unless overridden by session-level or unit-level diagnostic settings.

To view and configure application-level diagnostic settings:

1. Enter the following URL in a Web browser to open the Application-Level Diagnostic Settings window:

   `http://host_name:port_number/oiddas/ui/oracle/ldap/das/pages/Application`

   This window is described in "Application-Level Diagnostic Settings" on page A-10

2. Basic application-level configuration settings display in the Information section and connection pool settings and statistics display in the Connection Pool section.

   To display diagnostic information:

   a. In the **Configuration** section, change the **Value** field to **On**.

   b. Select **Update**. Scroll to the bottom of the Web page to view the diagnostic information.

   To change logging levels:

   a. In the **Logging** section, click the check boxes of the logging levels you want to change.

   b. Select a desired value from the **Change log level to** box.

   c. Select **Update**.

## Viewing and Configuring Session-Level Diagnostic Settings

You can view and configure session-level diagnostic settings for the current user session and for all units in an Oracle Delegated Administration Services application. Diagnostic settings can be turned on or off or can inherit application-level diagnostic

settings. If a session-level diagnostic setting is turned on, diagnostics will display, unless overridden by a unit-level diagnostic setting. If a session-level diagnostic setting is turned off, diagnostics will not display, unless overridden by a unit-level diagnostic setting. If a particular diagnostic setting is set to "inherit", then the application-level diagnostic setting applies.

To view and configure session-level diagnostic settings:

1. Enter the following URL in a Web browser to open the Session Level Diagnostic Settings window:

   `http://host_name:port_number/oiddas/ui/oracle/ldap/das/pages/Session`

   This window is described in Session Level Diagnostic Settings on page A-24

2. Basic session-level configuration settings display in the Information section and console navigation settings display in the Navigation section.

   To change session-level diagnostic settings:

   a. In the **Configuration** section, select a desired value in the Value field for the diagnostic setting you want to change.

   b. Select **Update**.

## Setting Unit-Level Diagnostic Settings

Unit-level diagnostic settings control the display of diagnostics for the current user session in a given unit. Applicable values for a diagnostic setting at the unit level are "on", "off", and "inherit". If a unit-level diagnostic setting is turned on, diagnostics will display for the specified unit. If a unit-level diagnostic setting is turned off, diagnostics will not display for the specified unit. If a value of "inherit" is applied to a diagnostic setting, then the session-level diagnostic setting applies.

To enable or disable diagnostics for the current user session and a specific unit, append a question mark and "diagnostic=on", or "diagnostic=off", or "diagnostic=inherit" to the URL of the desired unit. For example, the following URL enables diagnostics for the current user session with the user search unit:

```
http://host_name:port_number/oiddas/ui/oracle/ldap/das/
pages/UserSearch?diagnostic=on
```

## Diagnosing Login Problems

For problems logging in, examine the $*ORACLE_HOME*/ldap/log/das.log file. Also, verify the following:

- The URL contains the correct infrastructure host name and HTTP server port.
- You are using the correct redirection URL.
- You can successfully execute `ping` and `nslookup` commands from the Web client server to the infrastructure server.
- You can execute `ldapbind` commands from both administrative and user accounts.
- Whether a specific set of users is failing to log in.
- If any user accounts are locked.

> **See Also:** *Oracle Internet Directory Administrator's Guide* for information on password policies in Oracle Internet Directory

Also, verify that the following properties are correctly set in the $*ORACLE_HOME*/config/ias.properties file:

- DAS.LaunchSuccess
- IASname
- InfrastructureUse
- OIDhost
- OIDport
- OIDsslport
- VirtualHostName
- InfrastructureDBCommonName

Finally, ensure that the OC4J_SECURITY information in $*ORACLE_HOME*/opmn/conf/opmn.xml file is set correctly. The OC4J_SECURITY information is located in the following elements in the opmn.xml file:

```
<process-type id="OC4J_SECURITY" module-id="OC4J">
  <environment>
    <variable id="DISPLAY" value="Infrahost.us.oracle.com:0.0"/>
    <variable id="LD_LIBRARY_PATH" value="/app/oracle/product/10g/infra/lib"/>
  </environment>
  <module-data>
    <category id="start-parameters">
      <data id="java-options" value="-Djava.security.policy=/app/oracle/product
        /10g/infra/j2ee/OC4J_SECURITY/config/java2.policy -Djava.awt.headless=true
        -Xmx512m -Djava.awt.headless=true "/>
      <data id="oc4j-options" value="-properties"/>
    </category>
    <category id="stop-parameters">
      <data id="java-options" value="-Djava.security.policy=/app/oracle/product/
        10g/infra/j2ee/OC4J_SECURITY/config/java2.policy
        -Djava.awt.headless=true"/>
    </category>
  </module-data>
  <start timeout="900" retry="2"/>
  <stop timeout="120"/>
  <restart timeout="720" retry="2"/>
  <port id="ajp" range="3301-3400"/>
  <port id="rmi" range="3201-3300"/>
  <port id="jms" range="3701-3800"/>
  <process-set id="default_island" numprocs="1"/>
</process-type>
```

> **See Also:** *Oracle Application Server Single Sign-On Administrator's Guide* for additional information on how to resolve login problems

## Users Prompted to Change Password Multiple Times

Oracle Internet Directory  enables you to establish a password policy in which users are prompted to change their passwords after initial login. Users must change their

passwords by using the Oracle Internet Directory Self-Service Console Password Change screen. Using other mechanisms may not satisfy the password change requirement, and users may be prompted to change their password again the next time they log in.

> **See Also:** *Oracle Internet Directory Administrator's Guide* for information on password policies in Oracle Internet Directory

## Missing User Entries

User entries in Oracle Internet Directory that do not belong to the `inetOrgPerson` object class will not appear in the Self-Service Console. You can assign user entries to an object class by using Oracle Directory Manager or the `ldapmodify` command.

> **See Also:** The *Oracle Internet Directory Administrator's Guide* for information on how to use Oracle Directory Manager and the `ldapmodify` command

## Interpreting Error Messages

This section describes the error messages you may encounter with the Self-Service Console.

**500 Internal Server Error**

**Cause:** Usually indicates that Oracle Delegated Administration Services has not been started correctly.

**Action:** Follow the instructions in "Installing and Configuring Oracle Delegated Administration Services" on page 1-4 to determine whether Oracle Delegated Administration Services is running. Also, examine the $*ORACLE_HOME*/ldap/log/das.log file to determine what is causing the error.

**Warning: Page has Expired**

**Cause:** Some Oracle Delegated Administration Services pages use the POST method to submit HTTP requests. Clicking the Back button to view a page that has been submitted with the POST method usually results in a warning message from the Web browser that the page has expired. In general, use of the back button on DAS pages is discouraged.

**Action:** Avoid using the Web browser's Back button. Instead, use the Go Back button or other navigation buttons and links that appear in the Self-Service Console.

**Error: Cannot proceed. Please contact your Administrator to have your password reset!**

**Cause:** This error occurs if a user attempts to reset their password before specifying a password hint.

**Action:** An administrator must reset the user's password by following the instructions in "Changing the Password of a User" on page 5-10. To prevent this error from occurring again, the user must then specify a password hint by following the instructions in "Changing Your Own Password and Password Hint" on page 4-2.

# Diagnosing Service Unit Problems

Oracle Delegated Administration Services consists of a set of pre-defined, Web-based service units for performing directory operations on behalf of users. These units enable directory users to update their own information. This section contains these topics:

- Handling with Pop-Up Window Blocking
- Handling Cross-Domain Invocation Issues

---

**See Also:** *Oracle Identity Management Application Developer's Guide* for additional information on how to write custom applications to resolve the issues discussed in this section

---

## Handling with Pop-Up Window Blocking

When an Oracle Delegated Administration Services service unit tries to open a new Web browser window, the new window may not open if pop-up window blocking is enabled on a client's Web browser. To avoid pop-up window blocking, you need to write a custom application that opens a new window on a local application server, and then immediately redirects the page to the Oracle Delegated Administration Services service unit.

## Handling Cross-Domain Invocation Issues

Oracle Delegated Administration Services service units that need to return parameters to a calling page may fail due to cross-domain JavaScript security restrictions. To avoid such problems, you must write a custom Oracle Internet Directory application.

## Troubleshooting SSO Login Issues

When logging in to the Self-Service Console, the Web browser displays an error message that the server cannot be found. This occurs if the SSO service is down or if the `mod_osso` service is not configured properly. To resolve this issue, restart the SSO service or reconfigure the `mod_osso` service. For more information, refer to the *Oracle Application Server Single Sign-On Administrator's Guide*.

# Need More Help?

In case the information in the previous sections was not sufficient, you can find more solutions on Oracle*MetaLink*, `http://metalink.oracle.com`. If you do not find a solution for your problem, log a service request.

**See Also:**

- *Oracle Application Server Release Notes*, available on the Oracle Technology Network: `http://www.oracle.com/technology/documentation/index.html`

# Glossary

**access control item (ACI)**

An attribute that determines who has what type of access to what directory data. It contains a set of rules for structural access items, which pertain to entries, and content access items, which pertain to attributes. Access to both structural and content access items may be granted to one or more users or groups.

**access control list (ACL)**

The group of access directives that you define. The directives grant levels of access to specific data for specific clients, or groups of clients, or both.

**access control policy point**

An entry that contains security directives that apply downward to all entries at lower positions in the **directory information tree (DIT)**.

**ACI**

See **access control item (ACI)**.

**ACL**

See **access control list (ACL)**.

**ACP**

See **access control policy point**.

**administrative area**

A subtree on a directory server whose entries are under the control (schema, ACL, and collective attributes) of a single administrative authority.

**advanced symmetric replication (ASR)**

See **Oracle Database Advanced Replication**

**anonymous authentication**

The process by which the directory authenticates a user without requiring a user name and password combination. Each anonymous user then exercises the privileges specified for anonymous users.

**API**

See **application program interface**.

### application program interface

Programs to access the services of a specified application. For example, LDAP-enabled clients access directory information through programmatic calls available in the LDAP API.

### ASR

See **Oracle Database Advanced Replication**

### attribute

An item of information that describes some aspect of an entry. An entry comprises a set of attributes, each of which belongs to an **object class**. Moreover, each attribute has both a *type*, which describes the kind of information in the attribute, and a *value*, which contains the actual data.

### attribute configuration file

In an Oracle Directory Integration Platform environment, a file that specifies attributes of interest in a connected directory.

### attribute type

The kind of information an attribute contains, for example, `jobTitle`.

### attribute uniqueness

An Oracle Internet Directory feature that ensures that no two specified attributes have the same value. It enables applications synchronizing with the enterprise directory to use attributes as unique keys.

### attribute value

The particular occurrence of information appearing in that entry. For example, the value for the `jobTitle` attribute could be `manager`.

### authentication

The process of verifying the identity of a user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in a system.

### authorization

Permission given to a user, program, or process to access an object or set of objects.

### binding

The process of authenticating to a directory.

### central directory

In an Oracle Directory Integration Platform environment, the directory that acts as the central repository. In an Oracle Directory Integration Platform environment, Oracle Internet Directory is the central directory.

### certificate

An ITU x.509 v3 standard data structure that securely binds an identity to a public key. A certificate is created when an entity's public key is signed by a trusted identity: a **certificate authority (CA)**. This certificate ensures that the entity's information is correct and that the public key actually belongs to that entity.

### certificate authority (CA)

A trusted third party that certifies that other entities—users, databases, administrators, clients, servers—are who they say they are. The certificate authority verifies the user's identity and grants a certificate, signing it with the certificate authority's private key.

### certificate chain

An ordered list of certificates containing an end-user or subscriber certificate and its certificate authority certificates.

### change logs

A database that records changes made to a directory server.

### cipher suite

In SSL, a set of authentication, encryption, and data integrity algorithms used for exchanging messages between network nodes. During an SSL handshake, the two nodes negotiate to see which cipher suite they will use when transmitting messages back and forth.

### cluster

A collection of interconnected usable whole computers that is used as a single computing resource. Hardware clusters provide high availability and scalability.

### cold backup

The procedure to add a new **DSA** node to an existing replicating system by using the database copy procedure.

### concurrency

The ability to handle multiple requests simultaneously. Threads and processes are examples of concurrency mechanisms.

### concurrent clients

The total number of clients that have established a session with Oracle Internet Directory.

### concurrent operations

The number of operations that are being executed on the directory from all of the concurrent clients. Note that this is not necessarily the same as the concurrent clients, because some of the clients may be keeping their sessions idle.

### configset

See **configuration set entry**.

### configuration set entry

A directory entry holding the configuration parameters for a specific instance of the directory server. Multiple configuration set entries can be stored and referenced at runtime. The configuration set entries are maintained in the subtree specified by the subConfigsubEntry attribute of the DSE, which itself resides in the associated **directory information base (DIB)** against which the servers are started.

### connect descriptor

A specially formatted description of the destination for a network connection. A connect descriptor contains destination service and network route information.

The destination service is indicated by using its service name for the Oracle Database or its Oracle System Identifier (SID) for Oracle release 8.0 or version 7 databases. The network route provides, at a minimum, the location of the listener through use of a network address.

### connected directory

In an Oracle Directory Integration Platform environment, an information repository requiring full synchronization of data between Oracle Internet Directory and itself—for example, an Oracle human Resources database.

### consumer

A directory server that is the destination of replication updates. Sometimes called a slave.

### contention

Competition for resources.

### context prefix

The **DN** of the root of a **naming context**.

### cryptography

The practice of encoding and decoding data, resulting in secure messages.

### data integrity

The guarantee that the contents of the message received were not altered from the contents of the original message sent.

### decryption

The process of converting the contents of an encrypted message (ciphertext) back into its original readable format (plaintext).

### default knowledge reference

A **knowledge reference** that is returned when the base object is not in the directory, and the operation is performed in a naming context not held locally by the server. A default knowledge reference typically sends the user to a server that has more knowledge about the directory partitioning arrangement.

### default identity management realm

In a hosted environment, one enterprise—for example, an application service provider—makes Oracle components available to multiple other enterprises and stores information for them. In such hosted environments, the enterprise performing the hosting is called the default identity management realm, and the enterprises that are hosted are each associated with their own identity management realm in the DIT.

### default realm location

An attribute in the root Oracle Context that identifies the root of the default identity management realm.

### delegated administrator

In a hosted environment, one enterprise—for example, an application service provider—makes Oracle components available to multiple other enterprises and stores information for them. In such an environment, a global administrator performs activities that span the entire directory. Other administrators—called delegated

administrators—may exercise roles in specific identity management realms, or for specific applications.

### DES

Data Encryption Standard, a block cipher developed by IBM and the U.S. government in the 1970's as an official standard.

### DIB

See **directory information base (DIB)**.

### directory information base (DIB)

The complete set of all information held in the directory. The DIB consists of entries that are related to each other hierarchically in a **directory information tree (DIT)**.

### directory information tree (DIT)

A hierarchical tree-like structure consisting of the DNs of the entries.

### directory integration profile

In an Oracle Directory Integration Platform environment, an entry in Oracle Internet Directory that describes how Oracle Directory Integration Platform communicates with external systems and what is communicated.

### directory integration server

In an Oracle Directory Integration Platform environment, the server that drives the synchronization of data between Oracle Internet Directory and a **connected directory**.

### directory naming context

See **naming context**.

### directory provisioning profile

A special kind of **directory integration profile** that describes the nature of provisioning-related notifications that Oracle Directory Integration Platform sends to the directory-enabled applications

### directory replication group (DRG)

The directory servers participating in a replication agreement.

### directory server instance

A discrete invocation of a directory server. Different invocations of a directory server, each started with the same or different configuration set entries and startup flags, are said to be different directory server instances.

### directory-specific entry (DSE)

An entry specific to a directory server. Different directory servers may hold the same DIT name, but have different contents—that is, the contents can be specific to the directory holding it. A DSE is an entry with contents specific to the directory server holding it.

### directory synchronization profile

A special kind of **directory integration profile** that describes how synchronization is carried out between Oracle Internet Directory and an external system.

### directory system agent (DSA)

The X.500 term for a directory server.

### distinguished name (DN)

The unique name of a directory entry. It comprises all of the individual names of the parent entries back to the root.

### DIS

See **directory integration server**

### DIT

See **directory information tree (DIT)**

### DN

See **distinguished name (DN)**

### DRG

See **directory replication group (DRG)**

### DSA

See **directory system agent (DSA)**

### DSE

See **directory-specific entry (DSE)**

**DSA**-specific entries. Different DSAs may hold the same DIT name, but have different contents. That is, the contents can be specific to the DSA holding it. A DSE is an entry with contents specific to the DSA holding it.

### encryption

The process of disguising the contents of a message and rendering it unreadable (ciphertext) to anyone but the intended recipient.

### entry

The building block of a directory, it contains information about an object of interest to directory users.

### export agent

In an Oracle Directory Integration Platform environment, an agent that exports data out of Oracle Internet Directory.

### export data file

In an Oracle Directory Integration Platform environment, the file that contains data exported by an **export agent**.

### export file

See **export data file**.

### external agent

A directory integration agent that is independent of Oracle directory integration and provisioning server. Oracle directory integration and provisioning server does not provide scheduling, mapping, or error handling services for it. An external agent is

typically used when a third party metadirectory solution is integrated with the Oracle Directory Integration Platform.

### failover

The process of failure recognition and recovery. In an Oracle Application Server Cold Failover Cluster (Identity Management), an application running on one cluster node is transparently migrated to another cluster node. During this migration, clients accessing the service on the cluster see a momentary outage and may need to reconnect once the failover is complete.

### fan-out replication

Also called a point-to-point replication, a type of replication in which a supplier replicates directly to a consumer. That consumer can then replicate to one or more other consumers. The replication can be either full or partial.

### filter

A method of qualifying data, usually data that you are seeking. Filters are always expressed as DNs, for example: `cn=susie smith,o=acme,c=us`.

### global administrator

In a hosted environment, one enterprise—for example, an application service provider—makes Oracle components available to multiple other enterprises and stores information for them. In such an environment, a global administrator performs activities that span the entire directory.

### global unique identifier (GUID)

An identifier generated by the system and inserted into an entry when the entry is added to the directory. In a multimaster replicated environment, the GUID, not the DN, uniquely identifies an entry. The GUID of an entry cannot be modified by a user.

### grace login

A login occurring within the specified period before password expiration.

### group search base

In the Oracle Internet Directory default DIT, the node in the identity management realm under which all the groups can be found.

### guest user

One who is not an anonymous user, and, at the same time, does not have a specific user entry.

### GUID

See **global unique identifier (GUID)**.

### handshake

A protocol two computers use to initiate a communication session.

### hash

A number generated from a string of text with an algorithm. The hash value is substantially smaller than the text itself. Hash numbers are used for security and for faster access to data.

### identity management

The process by which the complete security life cycle for network entities is managed in an organization. It typically refers to the management of an organization's application users, where steps in the security life cycle include account creation, suspension, privilege modification, and account deletion. The network entities managed may also include devices, processes, applications, or anything else that needs to interact in a networked environment. Entities managed by an identity management process may also include users outside of the organization, for example customers, trading partners, or Web services.

### identity management realm

A collection of identities, all of which are governed by the same administrative policies. In an enterprise, all employees having access to the intranet may belong to one realm, while all external users who access the public applications of the enterprise may belong to another realm. An identity management realm is represented in the directory by a specific entry with a special object class associated with it.

### identity management realm-specific Oracle Context

An Oracle Context contained in each identity management realm. It stores the following information:

- User naming policy of the identity management realm—that is, how users are named and located
- Mandatory authentication attributes
- Location of groups in the identity management realm
- Privilege assignments for the identity management realm—for example: who has privileges to add more users to the Realm.
- Application specific data for that Realm including authorizations

### import agent

In an Oracle Directory Integration Platform environment, an agent that imports data into Oracle Internet Directory.

### import data file

In an Oracle Directory Integration Platform environment, the file containing the data imported by an **import agent**.

### inherit

When an object class has been derived from another class, it also derives, or inherits, many of the characteristics of that other class. Similarly, an attribute subtype inherits the characteristics of its supertype.

### instance

See **directory server instance**.

### integrity

The guarantee that the contents of the message received were not altered from the contents of the original message sent.

### Internet Engineering Task Force (IETF)

The principal body engaged in the development of new Internet standard specifications. It is an international community of network designers, operators,

vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.

### Internet Message Access Protocol (IMAP)

A protocol allowing a client to access and manipulate electronic mail messages on a server. It permits manipulation of remote message folders, also called mailboxes, in a way that is functionally equivalent to local mailboxes.

### key

A string of bits used widely in cryptography, allowing people to encrypt and decrypt data; a key can be used to perform other mathematical operations as well. Given a cipher, a key determines the mapping of the plaintext to the ciphertext.

### key pair

A **public key** and its associated **private key**.

See **public/private key pair**.

### knowledge reference

The access information (name and address) for a remote **DSA** and the name of the **DIT** subtree that the remote DSA holds. Knowledge references are also called referrals.

### latency

The time a client has to wait for a given directory operation to complete. Latency can be defined as wasted time. In networking discussions, latency is defined as the travel time of a packet from source to destination.

### LDAP

See **Lightweight Directory Access Protocol (LDAP)**.

### LDIF

See **LDAP Data Interchange Format (LDIF)**.

### Lightweight Directory Access Protocol (LDAP)

A standard, extensible directory access protocol. It is a common language that LDAP clients and servers use to communicate. The framework of design conventions supporting industry-standard directory products, such as the Oracle Internet Directory.

### LDAP Data Interchange Format (LDIF)

The set of standards for formatting an input file for any of the LDAP command-line utilities.

### logical host

In an Oracle Application Server Cold Failover Cluster (Identity Management), one or more disk groups and pairs of host names and IP addresses. It is mapped to a physical host in the cluster. This physical host impersonates the host name and IP address of the logical host

### man-in-the-middle

A security attack characterized by the third-party, surreptitious interception of a message. The third-party, the *man-in-the-middle*, decrypts the message, re-encrypts it (with or without alteration of the original message), and retransmits it to the

originally-intended recipient—all without the knowledge of the legitimate sender and receiver. This type of security attack works only in the absence of **authentication**.

### mapping rules file

In an Oracle Directory Integration Platform environment, the file that specifies mappings between Oracle Internet Directory attributes and those in a **connected directory**.

### master definition site (MDS)

In replication, a master definition site is the Oracle Internet Directory database from which the administrator runs the configuration scripts.

### master site

In replication, a master site is any site other than the master definition site that participates in LDAP replication.

### matching rule

In a search or compare operation, determines equality between the attribute value sought and the attribute value stored. For example, matching rules associated with the `telephoneNumber` attribute could cause "(650) 123-4567" to be matched with either "(650) 123-4567" or "6501234567" or both. When you create an attribute, you associate a matching rule with it.

### MD4

A one-way hash function that produces a 128-bit hash, or message digest. If as little as a single bit value in the file is modified, the MD4 checksum for the file will change. Forgery of a file in a way that will cause MD4 to generate the same result as that for the original file is considered extremely difficult.

### MD5

An improved version of MD4.

### MDS

See **master definition site (MDS)**

### metadirectory

A directory solution that shares information between all enterprise directories, integrating them into one virtual directory. It centralizes administration, thereby reducing administrative costs. It synchronizes data between directories, thereby ensuring that it is consistent and up-to-date across the enterprise.

### MTS

See **shared server**

### multimaster replication

Also called peer-to-peer or *n*-way replication, a type of replication that enables multiple sites, acting as equals, to manage groups of replicated data. In a multimaster replication environment, each node is both a supplier and a consumer node, and the entire directory is replicated on each node.

### naming attribute

The attribute used to compose the RDN of a new user entry created through Oracle Delegated Administration Services or Oracle Internet Directory Java APIs. The default value for this is `cn`.

### naming context

A subtree that resides entirely on one server. It must be contiguous, that is, it must begin at an entry that serves as the top of the subtree, and extend downward to either leaf entries or **knowledge reference**s (also called referrals) to subordinate naming contexts. It can range in size from a single entry to the entire DIT.

### native agent

In an Oracle Directory Integration Platform environment, an agent that runs under the control of the **directory integration server**. It is in contrast to an **external agent**.

### net service name

A simple name for a service that resolves to a connect descriptor. Users initiate a connect request by passing a user name and password along with a net service name in a connect string for the service to which they wish to connect:

```
CONNECT username/password@net_service_name
```

Depending on your needs, net service names can be stored in a variety of places, including:

- Local configuration file, `tnsnames.ora`, on each client
- Directory server
- Oracle Names server
- External naming service, such as NDS, NIS or CDS

### nickname attribute

The attribute used to uniquely identify a user in the entire directory. The default value for this is `uid`. Applications use this to resolve a simple user name to the complete distinguished name. The user nickname attribute cannot be multi-valued—that is, a given user cannot have multiple nicknames stored under the same attribute name.

### object class

A named group of attributes. When you want to assign attributes to an entry, you do so by assigning to that entry the object classes that hold those attributes.

All objects associated with the same object class share the same attributes.

### OEM

See **Oracle Enterprise Manager**.

### OID Control Utility

A command-line tool for issuing run-server and stop-server commands. The commands are interpreted and executed by the **OID Monitor** process.

### OID Database Password Utility

The utility used to change the password with which Oracle Internet Directory connects to an Oracle database.

### OID Monitor

The Oracle Internet Directory component that initiates, monitors, and terminates the Oracle directory server processes. It also controls the replication server if one is installed, and Oracle directory integration and provisioning server.

### one-way function

A function that is easy to compute in one direction but quite difficult to reverse compute, that is, to compute in the opposite direction.

### one-way hash function

A **one-way function** that takes a variable sized input and creates a fixed size output.

### Oracle Call Interface (OCI)

An application programming interface (API) that enables you to create applications that use the native procedures or function calls of a third-generation language to access an Oracle database server and control all phases of SQL statement execution.

### Oracle Delegated Administration Services

A set of individual, pre-defined services—called Oracle Delegated Administration Services units—for performing directory operations on behalf of a user. Oracle Internet Directory Self-Service Console makes it easier to develop and deploy administration solutions for both Oracle and third-party applications that use Oracle Internet Directory.

### Oracle Directory Integration Platform

A component of **Oracle Internet Directory**. It is a framework developed to integrate applications around a central LDAP directory like Oracle Internet Directory.

### Oracle directory integration and provisioning server

In an Oracle Directory Integration Platform environment, a daemon process that monitors Oracle Internet Directory for change events and takes action based on the information present in the **directory integration profile**.

### Oracle Directory Manager

A Java-based tool with a graphical user interface for administering Oracle Internet Directory.

### Oracle Enterprise Manager

A separate Oracle product that combines a graphical console, agents, common services, and tools to provide an integrated and comprehensive systems management platform for managing Oracle products.

### Oracle Identity Management

An infrastructure enabling deployments to manage centrally and securely all enterprise identities and their access to various applications in the enterprise.

### Oracle Internet Directory

A general purpose directory service that enables retrieval of information about dispersed users and network resources. It combines Lightweight Directory Access Protocol (LDAP) Version 3 with the high performance, scalability, robustness, and availability of the Oracle Database.

### Oracle Net Services

The foundation of the Oracle family of networking products, allowing services and their client applications to reside on different computers and communicate. The main function of Oracle Net Services is to establish network sessions and transfer data between a client application and a server. Oracle Net Services is located on each computer in the network. Once a network session is established, Oracle Net Services acts as a data courier for the client and the server.

### Oracle PKI certificate usages

Defines Oracle application types that a **certificate** supports.

### Oracle Wallet Manager

A Java-based application that security administrators use to manage public-key security credentials on clients and servers.

See Also: *Oracle Advanced Security Administrator's Guide*

### Oracle Database Advanced Replication

A feature in the Oracle Database that enables database tables to be kept synchronized across two Oracle databases.

### other information repository

In an Oracle Directory Integration Platform environment, in which Oracle Internet Directory serves as the **central directory**, any information repository except Oracle Internet Directory.

### partition

A unique, non-overlapping directory naming context that is stored on one directory server.

### peer-to-peer replication

Also called multimaster replication or *n*-way replication. A type of replication that enables multiple sites, acting as equals, to manage groups of replicated data. In such a replication environment, each node is both a supplier and a consumer node, and the entire directory is replicated on each node.

### PKCS #12

A **public-key encryption** standard (PKCS). RSA Data Security, Inc. PKCS #12 is an industry standard for storing and transferring personal authentication credentials—typically in a format called a **wallet**.

### plaintext

Message text that has not been encrypted.

### point-to-point replication

Also called fan-out replication is a type of replication in which a supplier replicates directly to a consumer. That consumer can then replicate to one or more other consumers. The replication can be either full or partial.

### primary node

In an Oracle Application Server Cold Failover Cluster (Identity Management), the cluster node on which the application runs at any given time.

**See Also:** **secondary node** on page Glossary-16

### private key

In public-key cryptography, this key is the secret key. It is primarily used for decryption but is also used for encryption with digital signatures.

### provisioning agent

An application or process that translates Oracle-specific provisioning events to external or third-party application-specific events.

### provisioned applications

Applications in an environment where user and group information is centralized in Oracle Internet Directory. These applications are typically interested in changes to that information in Oracle Internet Directory.

### profile

See **directory integration profile**

### proxy user

A kind of user typically employed in an environment with a middle tier such as a firewall. In such an environment, the end user authenticates to the middle tier. The middle tier then logs into the directory on the end user's behalf. A proxy user has the privilege to switch identities and, once it has logged into the directory, switches to the end user's identity. It then performs operations on the end user's behalf, using the authorization appropriate to that particular end user.

### public key

In public-key cryptography this key is made public to all, it is primarily used for encryption but can be used for verifying signatures.

### public-key cryptography

Cryptography based on methods involving a public key and a private key.

### public-key encryption

The process in which the sender of a message encrypts the message with the public key of the recipient. Upon delivery, the message is decrypted by the recipient using the recipient's private key.

### public/private key pair

A mathematically related set of two numbers where one is called the private key and the other is called the public key. Public keys are typically made widely available, while private keys are available only to their owners. Data encrypted with a public key can only be decrypted with its associated private key and vice versa. Data encrypted with a public key cannot be decrypted with the same public key.

### realm search base

An attribute in the root Oracle Context that identifies the entry in the DIT that contains all identity management realms. This attribute is used when mapping a simple realm name to the corresponding entry in the directory.

### referral

Information that a directory server provides to a client and which points to other servers the client must contact to find the information it is requesting.

See also **knowledge reference**.

### relational database

A structured collection of data that stores data in tables consisting of one or more rows, each containing the same set of columns. Oracle makes it very easy to link the data in multiple tables. This is what makes Oracle a relational database management system, or RDBMS. It stores data in two or more tables and enables you to define relationships between the tables. The link is based on one or more fields common to both tables.

### replica

Each copy of a naming context that is contained within a single server.

### RDN

See **relative distinguished name (RDN)**.

### registry entry

An entry containing runtime information associated with invocations of Oracle directory servers, called a **directory server instance**. Registry entries are stored in the directory itself, and remain there until the corresponding directory server instance stops.

### relative distinguished name (RDN)

The local, most granular level entry name. It has no other qualifying entry names that would serve to uniquely address the entry. In the example, `cn=Smith,o=acme,c=US`, the RDN is `cn=Smith`.

### remote master site (RMS)

In a replicated environment, any site, other than the **master definition site (MDS)**, that participates in Oracle Database Advanced Replication.

### replication agreement

A special directory entry that represents the replication relationship among the directory servers in a **directory replication group (DRG)**.

### response time

The time between the submission of a request and the completion of the response.

### root DSE

See **root directory specific entry**.

### root directory specific entry

An entry storing operational information about the directory. The information is stored in a number of attributes.

### Root Oracle Context

In the Oracle Identity Management infrastructure, the Root Oracle Context is an entry in Oracle Internet Directory containing a pointer to the default identity management realm in the infrastructure. It also contains information on how to locate an identity management realm given a simple name of the realm.

### SASL

See **Simple Authentication and Security Layer (SASL)**

### scalability

The ability of a system to provide throughput in proportion to, and limited only by, available hardware resources.

### schema

The collection of attributes, object classes, and their corresponding matching rules.

### secondary node

In an Oracle Application Server Cold Failover Cluster (Identity Management), the cluster node to which an application is moved during a failover.

**See Also:** **primary node** on page Glossary-13

### Secure Hash Algorithm (SHA)

An algorithm that takes a message of less than 264 bits in length and produces a 160-bit message digest. The algorithm is slightly slower than MD5, but the larger message digest makes it more secure against brute-force collision and inversion attacks.

### Secure Socket Layer (SSL)

An industry standard protocol designed by Netscape Communications Corporation for securing network connections. SSL provides authentication, encryption, and data integrity using public key infrastructure (PKI).

### service time

The time between the initiation of a request and the completion of the response to the request.

### session key

A key for symmetric-key cryptosystems that is used for the duration of one message or communication session.

### SGA

See **System Global Area (SGA)**.

### SHA

See **Secure Hash Algorithm (SHA)**.

### shared server

A server that is configured to allow many user processes to share very few server processes, so the number of users that can be supported is increased. With shared server configuration, many user processes connect to a dispatcher. The dispatcher directs multiple incoming network session requests to a common queue. An idle shared server process from a shared pool of server processes picks up a request from the queue. This means a small pool of server processes can server a large amount of clients. Contrast with dedicated server.

### sibling

An entry that has the same parent as one or more other entries.

### simple authentication

The process by which the client identifies itself to the server by means of a DN and a password which are not encrypted when sent over the network. In the simple

authentication option, the server verifies that the DN and password sent by the client match the DN and password stored in the directory.

### Simple Authentication and Security Layer (SASL)

A method for adding authentication support to connection-based protocols. To use this specification, a protocol includes a command for identifying and authenticating a user to a server and for optionally negotiating a security layer for subsequent protocol interactions. The command has a required argument identifying a SASL mechanism.

### single key-pair wallet

A **PKCS #12**-format **wallet** that contains a single user **certificate** and its associated **private key**. The **public key** is imbedded in the certificate.

### slave

See **consumer**.

### SLAPD

Standalone LDAP daemon.

### smart knowledge reference

A **knowledge reference** that is returned when the knowledge reference entry is in the scope of the search. It points the user to the server that stores the requested information.

### specific administrative area

Administrative areas control:

- Subschema administration
- Access control administration
- Collective attribute administration

A *specific* administrative area controls one of these aspects of administration. A specific administrative area is part of an autonomous administrative area.

### sponsor node

In replication, the node that is used to provide initial data to a new node.

### SSL

See **Secure Socket Layer (SSL)**.

### subACLSubentry

A specific type of subentry that contains ACL information.

### subclass

An object class derived from another object class. The object class from which it is derived is called its **superclass**.

### subentry

A type of entry containing information applicable to a group of entries in a subtree. The information can be of these types:

- Access control policy points
- Schema rules

- Collective attributes

Subentries are located immediately below the root of an administrative area.

### subordinate reference

A knowledge reference pointing downward in the DIT to a naming context that starts immediately below an entry.

### subschema DN

The list of DIT areas having independent schema definitions.

### subSchemaSubentry

A specific type of **subentry** containing schema information.

### subtype

An attribute with one or more options, in contrast to that same attribute without the options. For example, a `commonName` (`cn`) attribute with American English as an option is a subtype of the `commonName` (`cn`) attribute without that option. Conversely, the `commonName` (`cn`) attribute without an option is the **supertype** of the same attribute with an option.

### super user

A special directory administrator who typically has full access to directory information.

### superclass

The object class from which another object class is derived. For example, the object class `person` is the superclass of the object class `organizationalPerson`. The latter, namely, `organizationalPerson`, is a **subclass** of `person` and inherits the attributes contained in `person`.

### superior reference

A knowledge reference pointing upward to a DSA that holds a naming context higher in the DIT than all the naming contexts held by the referencing DSA.

### supertype

An attribute without options, in contrast to the same attribute with one or more options. For example, the `commonName` (`cn`) attribute without an option is the supertype of the same attribute with an option. Conversely, a `commonName` (`cn`) attribute with American English as an option is a **subtype** of the `commonName` (`cn`) attribute without that option.

### supplier

In replication, the server that holds the master copy of the naming context. It supplies updates from the master copy to the **consumer** server.

### System Global Area (SGA)

A group of shared memory structures that contain data and control information for one Oracle database instance. If multiple users are concurrently connected to the same instance, the data in the instance SGA is shared among the users. Consequently, the SGA is sometimes referred to as the "shared global area." The combination of the background processes and memory buffers is called an Oracle instance.

### system operational attribute

An attribute holding information that pertains to the operation of the directory itself. Some operational information is specified by the directory to control the server, for example, the time stamp for an entry. Other operational information, such as access information, is defined by administrators and is used by the directory program in its processing.

### TLS

See **Transport Layer Security (TLS)**

### think time

The time the user is not engaged in actual use of the processor.

### throughput

The number of requests processed by Oracle Internet Directory for each unit of time. This is typically represented as "operations per second."

### Transport Layer Security (TLS)

A protocol providing communications privacy over the Internet. The protocol enables client/server applications to communicate in a way that prevents eavesdropping, tampering, or message forgery.

### trusted certificate

A third party identity that is qualified with a level of trust. The trust is used when an identity is being validated as the entity it claims to be. Typically, the certificate authorities you trust issue user certificates.

### trustpoint

See **trusted certificate**.

### UTF-16

16-bit encoding of **Unicode**.The Latin-1 characters are the first 256 code points in this standard.

### Unicode

A type of universal character set, a collection of 64K characters encoded in a 16-bit space. It encodes nearly every character in just about every existing character set standard, covering most written scripts used in the world. It is owned and defined by Unicode Inc. Unicode is canonical encoding which means its value can be passed around in different locales. But it does not guarantee a round-trip conversion between it and every Oracle character set without information loss.

### UNIX Crypt

The UNIX encryption algorithm.

### user search base

In the Oracle Internet Directory default DIT, the node in the identity management realm under which all the users are placed.

### UTC (Coordinated Universal Time)

The standard time common to every place in the world. Formerly and still widely called Greenwich Mean Time (GMT) and also World Time, UTC nominally reflects the

mean solar time along the Earth's prime meridian. UTC is indicated by a z at the end of the value, for example, 200011281010z.

### UTF-8

A variable-width 8-bit encoding of **Unicode** that uses sequences of 1, 2, 3, or 4 bytes for each character. Characters from 0-127 (the 7-bit ASCII characters) are encoded with one byte, characters from 128-2047 require two bytes, characters from 2048-65535 require three bytes, and characters beyond 65535 require four bytes. The Oracle character set name for this is AL32UTF8 (for the Unicode 3.1 standard).

### virtual host name

In an Oracle Application Server Cold Failover Cluster (Identity Management), the host name corresponding to this virtual IP address.

### virtual IP address

In an Oracle Application Server Cold Failover Cluster (Identity Management), each physical node has its own physical IP address and physical host name. To present a single system image to the outside world, the cluster uses a dynamic IP address that can be moved to any physical node in the cluster. This is called the virtual IP address.

### wallet

An abstraction used to store and manage security credentials for an individual entity. It implements the storage and retrieval of credentials for use with various cryptographic services. A wallet resource locator (WRL) provides all the necessary information to locate the wallet.

### wait time

The time between the submission of the request and initiation of the response.

### X.509

A popular format from ISO used to sign public keys.

# Index

## A



## B



## C



## D

## E



## G



## H



## I



## J



## L



## M



## O

## P



## R



## S

## T



## U



## V