# Oracle® Internet Directory

Release Notes

Release 9.0.2.1.0 for Windows NT

May 2002

**Part No. A97633-01**

This document summarizes the differences between Oracle Internet Directory and its documented functionality.

**See Also:** *Oracle9i Application Server Release Notes*

These release notes contain these topics:

- Introduction
- Installation Process
- New Features
- Oracle Internet Directory Server Release 9.0.2.1.0
- Oracle Internet Directory Client Release 9.0.2.1.0

## 1 Introduction

### 1.1 About Oracle Internet Directory

Oracle Internet Directory Release 9.0.2.1.0 is an LDAP-v3 compliant directory server that is powered by theOracle9*i* Database Server. It is a component of Oracle9*i* Application Server (9.0.2.1.0) and exploits the Oracle RDBMS technology to achieve scalability and sophisticated data management.

There are two installable components of Oracle Internet Directory:

- Oracle Internet Directory Client 9.0.2.1.0

  This component installs the LDAP client, the Oracle Directory Integration Platform, and the administration tools required for

accessing and managing data in Oracle Internet Directory remotely. The files included in the client installation are a subset of those installed as part of the server installation.

- Oracle Internet Directory Server 9.0.2.1.0

  This component includes:

  - The directory server and all related components
  - All components included with the client installation

### 1.2 About These Release Notes

These release notes are relevant only to Oracle Internet Directory Release 9.0.2.1.0 and its integral components. They document any differences between the shipped software (and its integral parts) and its documented functionality, as well as fixed bugs, and known problems and workarounds.

## 2 Installation Process

To install Oracle Internet Directory Release 9.0.2.1.0, select the Oracle9*i*AS Infrastructure 9.0.2.1.0 Installation type.

For more information, please see the appropriate installation or migration documentation for Oracle9*i* Application Server.

### 2.1 Post-Installation/Post-Upgrade Step

At the end of a new installation it is recommended that the $ORACLE_HOME/ldap/admin/oidstats.sh be executed. Otherwise, the OID server performance might be affected. The usage is as follows:

`$ORACLE_HOME/ldap/admin/oidstats.sh -connect` *`Database_connect_string`* `-all -pct` *`Percent_of_Data_to_sample`*—for example, 100

In case of upgrade, if you observe deterioration in the server performance, then you need to run the oidstats.sh tool as mentioned above. Please note, the amount of time this script takes to complete its task is dependent on the directory size.

## 2.2 Additional Post-Upgrade Task to Create spfile for the Oracle Internet Directory Database

The `spfile.ora` needs to be created from the `init.ora` file. This can be done by connecting to the database as SYSDBA and running the following SQL command:

```
create spfile="spfile_name" FROM pfile="source_init.ora";
```

In the above command,

<spfile name>: spfile<ORACLE_SID>.ora

<source init.ora>: init<ORACLE_SID>.ora

## 2.3 Default Directory Information Tree Created During Oracle Internet Directory Installation

In this release, the following directory information tree elements are created by default:

- Root Oracle Context: `cn=OracleContext`. This is the container where Oracle products store enterprise-wide configuration data.
- Default Subscriber: `dc=dns_domain_of_computer,dc=com`. This is an approximation of the enterprise DIT structure. This is the container under which Oracle products expect to find users and groups in the enterprise. For example, if Oracle Internet Directory is being installed on a computer whose hostname is: computer1.us.acme.com, then the default subscriber tree created by Oracle Internet Directory installation would be `dc=acme,dc=com`. Oracle products expect to find all users under the container `cn=users,dc=acme,dc=com` and all groups under `cn=groups,dc=acme,dc=com`. In addition to creating the default subscriber entry, OID Configuration Assistant stores a pointer to it in the Root Oracle Context so that other Oracle Internet Directory enabled components can bootstrap themselves.

For enterprises that have already rolled out a directory, the default subscriber may not match the actual enterprise directory information tree requirements. For example, if a company wants to store all of its users in a different container like `o=acme,c=us`, then the default tree created by Oracle Internet Directory installation is not sufficient. In order to designate an alternate entry in Oracle Internet Directory as the default subscriber, you must perform the following tasks

- Install OID
- Create Enterprise Specific Directory tree using command line tools or OIDADMIN

- Run OIDCA in a special mode to configure the Enterprise Specific Directory Entry as a the default subscriber. Here are the arguments to OIDCA.

```
$ORACLE_HOME/bin/oidca
/createDefaultSubscriber
[/help] - optional to show usage
/host OID_host
/port <OID_port>
/userDN <bindDN>
/userPwd <bindDN_password>
/subscriberDN <subscriber_DN_to_be_turned_into_a_default_subscriber>
```

## 2.4 Instructions for Manually Deploying the Delegated Administration Service

The Delegated Administration Service (DAS) is deployed automatically in the infrastructure installation. In some situations, there may be a requirement to deploy it on a host other than that on which the infrastructure is deployed. To deploy the Delegated Administration Service on a different computer where the middle tier is installed, perform the following steps:

1. Verify that the computer has at least the core installation installed and the installation is pointing to an existing Oracle Internet Directory / SSO.
2. Navigate to the *ORACLE_HOME*/dcm/bin directory.
3. Create a new component using the following command:

```
dcmctl createcomponent -verbose -debug -ct oc4j -co OC4J_DAS
```

4. Start the component using the following command:

```
dcmctl start -verbose -debug -co OC4J_DAS
```

5. Deploy the DAS ear file using the following command:

```
dcmctl deployApplication -debug -verbose -a oiddas -f
ORACLE_HOME/ldap/das/oiddas.ear -co OC4J_DAS
```

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_DAS section of opmn.xml:

```
<environment>
<prop name="DISPLAY" value="%hostname%:0.0"/>
<prop name="LD_LIBRARY_PATH" value="%ORACLE_HOME%/lib"/>
</environment>
```

   Replace *hostname* and *ORACLE_HOME* with the appropriate values. Hostname should point to a computer where X server is running.

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

```
<oc4j maxRetry="3" instanceName="OC4J_DAS" gid="OC4J_DAS"
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="DISPLAY" value="sandal:0.0"/>
        <prop name="LD_LIBRARY_PATH" value="/home/ias902/lib"/>
          </environment>
</oc4j>
```

7. Navigate to the *ORACLE_HOME*/dcm/bin directory.

8. Save the changes to the repository using the following command:

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

9. Restart OPMN using the following command:

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

10. Stop and start OC4J_DAS instance using the following commands:

```
dcmctl stop -verbose -debug -ct oc4j -co OC4J_DAS
dcmctl start -verbose -debug -ct oc4j -co OC4J_DAS
```

# 3 New Features

## 3.1 New Feature List

The following major new features and capabilities of Oracle Internet Directory have been introduced since the release of Oracle9*i* Database Server Release 1:

- Oracle Directory Integration Platform
- Oracle Provisioning Integration Service
- iPlanet Connector
- Web-Based OID Server Manageability / Enterprise Manager User Interface
- Entry cache
- Support for a single Oracle Internet Directory instance to listen on both SSL and non-SSL ports.
- Support for multiple verifier attributes types
- Password policy management enhancements
- Access control list (ACL) and proxy-user enhancements
- Alias de-referencing
- Replication configuration enhancements
- Plug-in support
- Attribute uniqueness

## 3.2 New Feature Details

This section provides more detail about each of the enhanced features listed in Section 3.1"New Feature List".

Oracle Internet Directory enables customers to consolidate all of their users in an LDAP directory. It provides a single repository and administration environment for the creation and management of user accounts in an Oracle9*i* Application Server Release 2 (9.0.2) deployment. Oracle Internet Directory provides the backend for centralized user authentication, including for Oracle9*i*AS Single Sign-On.

In Oracle9*i* Application Server, the following components are Oracle Internet Directory-enabled:

- Oracle9*i*AS Single Sign-On
- Oracle9*i*AS Portal
- Oracle9*i*AS Containers for J2EE
- Oracle9*i*AS Dynamic Services, delivered as part of Oracle HTTP Server
- Oracle9*i*AS Forms Services
- Oracle9*i*AS Reports Services
- Oracle9*i*AS Unified Messaging
- Oracle Internet File System
- Oracle9*i*AS Internet Hosting Kit
- JAAS

### 3.2.1 Oracle Directory Integration Platform

Oracle Internet Directory Release 9.0.2.1.0 introduces new kinds of connectivity with other applications and repositories, both Oracle-built and otherwise. The new Oracle Provisioning Integration Service and Oracle Directory Synchronization Service are built upon the Oracle Directory Integration Platform (introduced with Oracle Internet Directory Release 2.1.1.1 in the Oracle8*i* Release 3 timeframe).

### 3.2.2 Oracle Provisioning Integration Service

Provisioning is the process of granting or revoking a user's access to application resources based on business rules. The user may be either a human end user or an application. The Oracle Provisioning Integration Service ensures that subscribing applications or business entities are alerted to updates in Oracle Internet Directory for the purpose of keeping local repositories synchronized. It enables you to synchronize local, application-specific information by using Oracle Internet Directory as a source of truth.

### 3.2.3 iPlanet Connector

Customers can synchronize the user data in Oracle Internet Directory with an iPlanet directory. The synchronization is bi-directional—that is, changes in Oracle Internet Directory are propagated to the iPlanet directory, and changes in iPlanet directory are propagated to Oracle Internet Directory. The attributes and entries to be synchronized can be configured at run time.

### 3.2.4 Web-Based Oracle Internet Directory Server Manageability/Enterprise Manager User Interface

Oracle Internet Directory Release 9.0.2.1.0 introduces a new graphic user interface tool, built on the Oracle Enterprise Manager Daemon (EMD) architecture, which enables instances of Oracle Internet Directory to be monitored from remote workstations where Oracle Enterprise Manager has been installed. This new server manageability tool enables stopping, starting, monitoring, and charting of LDAP directory server instances.

### 3.2.5 Server Entry Cache

This feature reduces directory query latency for LDAP clients. By configuring a server side entry cache based on naming context, identity of client, or other available parameters, Oracle Internet Directory ensures that previously retrieved entries and their attributes are stored in memory and are thus available to subsequent data requestors. Queries that conform to the configured parameters then need only retrieve a small subset of data-internal globally unique identifiers—for filter-matching entries from the directory. These returned identifiers are then used as a fast lookup mechanism into the cached entry and attribute data, which is then returned to the client.

### 3.2.6 Enterprise Password Policy Management Enhancements

You can now construct password policies to ensure:

- Expiration dates
- Grace periods
- Minimum password lengths
- Approved password syntaxes and retry limits
- Lockout of those attempting to gain illicit access to the directory service after a certain number of failed attempts

During upgrade from Release 9.0.1 to Release 9.0.2, the existing password policy entry is copied to the Root Oracle Context as well as the subscriber Oracle Context. The entities under Root Oracle Context are exempted from any kind of password policy. Oracle Internet Directory password policy can be enforced on a per-subscriber basis.

The password policy in the Subscriber Oracle Context, applies to the entire DIT, identified by the value of the `orclcommonusersearchbase` attribute, in the common entry under the subscriber oracle context. By default, this attribute is set to `cn=users,cn=DEFAULT_SUBSCRIBER,dc=com`. This means that all users underneath the container `cn=users,cn=DEFAULT_SUBSCRIBER, dc=com`, will be governed by

the Password Policy in the Subscriber Oracle Context. If the attribute `orclcommonusersearchbase`, is not present or deleted from the common entry under the Subscriber Oracle Context, then the policy under the Root Oracle Context applies to the entire subscriber DIT.

The `userpassword` attribute can hashed using one of these available hashing algorithms:

- MD4 - A one-way hash function that produces a 128-bit hash
- MD5 - An improved, and more complex, version of MD4
- SHA - Secure Hash Algorithm, which produces a 160-bit hash, longer than MD5. The algorithm is slightly slower than MD5, but the larger message digest makes it more secure against brute-force collision and inversion attacks. You can also use salted SHA. A salt is a random number added to and stored with the hash value. It prevents pre-computed dictionary attacks by making it extremely expensive to recover the value that was originally hashed.
- UNIX Crypt - The UNIX encryption algorithm
- NONE - No Hashing

Salted SHA and MD5 are supported only for the purpose of migrating data from other LDAP directories into Oracle Internet Directory. The generation of salted SHA and MD5 values is not supported. If existing passwords are hashed using salted SHA or MD5, then these values can be stored, as is, in Oracle Internet Directory without any user authentication failures.

### 3.2.7 Attribute Uniqueness

In the prior Oracle Internet Directory architecture, the only way to enforce attribute uniqueness was to make an attribute a part of your DN. This worked well with the user identifier (if used as the RDN), but it was not always appropriate and easy to configure. Within a level of a branch of the tree, it was guaranteed to be unique. For example, if your DN was uid=dlin, ou=people, o=oracle, then this would be unique directly under ou=people. However, you could have the same user identifier in another branch for example, uid=dlin, ou=others, o=oracle. In short, attribute uniqueness was guaranteed only under a given branch, and only within one level.

The applications Oracle Internet Directory synchronizes with can use attributes other than DN as their unique keys. The ability of Oracle Internet Directory to enforce attribute uniqueness enables all applications their own notions of "user," to synchronize their user base with a user repository stored in an enterprise Oracle Internet Directory server.

### 3.2.8 Multiple Password Verifier Support

Oracle Internet Directory can now store passwords for multiple applications and protocols. For example, four-digit Personal Identification Numbers (PINs) for voicemail can reside alongside longer alphanumeric single sign-on passwords and X509 v3 digital certificates for the same user. This new feature gives the application developer far greater flexibility for directory-enabling their product stack.

### 3.2.9 Expanded Proxy User Capabilities

This new feature enables a developer to exploit the power of the middle tier more effectively. Users no longer need to establish independent, unrelated sessions with the directory. If a middle-tier from Oracle9*i* Application Server or elsewhere invokes the proxy user bind method on behalf of numerous clients in succession, then Oracle Internet Directory respects the credential and privileges of each clients, even though the agent doing the actual binding remains unchanged throughout.

### 3.2.10 Oracle Directory Manager Enhancements

Oracle Internet Directory's standalone, 100% Java administration console, Oracle Directory Manager, has evolved in many ways. You can use it to:

- Configure hosted subscriber domains
- Construct password policies
- Configure Oracle Directory Synchronization Service and Oracle Internet Directory connectors and agents

In general, any directory-specific configuration or maintenance task that you cannot perform by using Oracle Enterprise Manager you can now perform by using Oracle Directory Manager, as well as command-line interfaces supplied with Oracle Internet Directory.

### 3.2.11 Server-Side Plug-in Framework

This new feature enables directory applications to roll out advanced capabilities such as referential integrity / cascading deletions of LDAP objects, external authentication of directory clients, brokered access, and synchronization with external relational tables. The plug-ins are executable before or after an LDAP command takes place, without the traditional risks of such technologies.

### 3.2.12 Entry Alias Dereferencing

The LDAP v3 standard requires that all entries in a directory have globally unique identifiers known as distinguished names. These are typically fairly long and cumbersome to use, so Oracle Internet Directory provides this

new feature to automatically dereference IETF-standard alias objects used to point to a fully-qualified LDAP distinguished name. For example, `DavesServer1` can be used as an entry alias or pointer to the actual directory entry named dc=server1, dc=us, dc=oracle, dc=com. Oracle Internet Directory stores, parses, and chases all alias references for complete client-side transparency.

### 3.2.13 Support for a Single Oracle Internet Directory Instance to Listen on Both SSL and Non-SSL Ports

In Oracle Internet Directory Release 9.0.2.1.0, a single instance of an Oracle Internet Directory server can listen on both SSL and non-SSL ports. This obviates the need to start two separate instances, one listening on an SSL port and the other on a non-SSL port.

### 3.2.14 Replication Configuration Enhancements

Oracle directory replication agreements can now be automatically setup, thereby simplifying replication server configuration.

# 4 Oracle Internet Directory Server Release 9.0.2.1.0

Oracle Internet Directory Release 9.0.2.1.0 includes all of the binaries required to run the directory server, the Oracle Directory Integration Platform, and associated components from an Oracle Home.

## 4.1 Database Compatibility

Oracle Internet Directory Release 9.0.2.1.0 is certified against Oracle9*i* Database Server Release 1 (9.0.1.2.0) only.

## 4.2 Client Compatibility

Oracle Directory Manager 9.0.2.1.0 is certified to work against Oracle Internet Directory Release 9.0.2.1.0 servers. Older versions of Oracle Directory Manager may also function against the new release of the server, but new functionality will not be accessible from these older clients.

## 4.3 Database Access Mechanisms

The database being used as the data store for Oracle Internet Directory should be dedicated for Oracle Internet Directory. Because Oracle Internet Directory itself accesses its backend database as a regular database user, using LDAP-enabled features in some other Oracle products can cause circular dependencies. Oracle Corporation recommends that you not use

the following database access mechanisms for Oracle Internet Directory database connections:

- Oracle Net LDAP naming, which allows Oracle Net Services clients to look up an LDAP server for resolving database service names. Using Oracle Net Services can prevent Oracle Internet Directory from starting.
- Enterprise Users and Roles—part of Oracle Advanced Security—which enables the database to refer to a directory server to determine which enterprise roles have been granted to a particular enterprise user. Oracle Internet Directory cannot login to its own database as an enterprise user.

## 4.4 Running Multiple Instances of the Directory Server

You can now run multiple instances of the directory server on the same computer, each in its own distinct *ORACLE_HOME* directory.

For example, one instance might be running in SSL mode while the other may be running in non-SSL mode (although with Oracle Internet Directory Release 9.0.2.1.0, separate instances are not necessary to do this).

If you are using the Oracle Internet Directory server software (binaries) on a computer other than the one where your database binaries are located, then all directory server instances using a given database instance must be co-located.

For example, running a directory server instance on Computer A and another on Computer B, both using a common SID defined on Computer C is not supported. However, running two distinct directory server instances on Computer A against a database on Computer B is supported.

Configurations as described above require two separate installations of the complete Oracle Internet Directory component on both the intended "LDAP server" computer and the "database" computer. On the LDAP server computer, the database installed with it is never used and, after installation, may be safely removed. On the database computer, the LDAP server binaries are never used and, after installation, may also be safely removed.

## 4.5 Oracle Directory Integration Platform Issues and Limitations

### 4.5.1 Starting Up The Oracle Directory Integration Server On Windows NT (Bug-2373878)

The Oracle directory integration server can be started only by the owner of the Oracle Directory Service which is running with the name of `Oracle`*`ORACLE_HOME_NAME`*`InternetDirectory` in any Oracle installation. By default, on NT all the services run with the credentials of a

user named system which is internal to NT.So, the owner of the Oracle Directory Service needs to be reset to the administrator/login_identifier authorized to run the Oracle directory and related services. After you do this, perform the following steps:

1. Configure a user with logon Service Privileges. This can be achieved by, Click on Start->settings->Control Panel
2. Click on Services.
3. Double click on `Oracle`*`ORACLE_HOME_NAME`*`InternetDirectory`, Service Window appears. In the "Logon as" section, select "this account."
4. Specify the login id and password and click OK.
5. Stop, then start the service.
6. Re-register the Directory Integration Server by running odisrvreg.
7. Start the directory Integration Server using oidctl.

### 4.5.2 Oracle Directory Integration Platform and Replication

If you use the Oracle Directory Integration Platform in a replicated environment consisting of more than one Oracle Internet Directory server nodes, then you must set the `orcldiprepository` attribute in the DSE root to `1`. This enables the server to generate the change log entries for changes coming from the other Oracle Internet Directory nodes. By default, the server does not generate these change log entries. The change log entries are required for directory data to be synchronized with third-party directories and metadirectories.

### 4.5.3 Binary Attributes Cannot Be Synchronized (bug 1692057)

Binary attributes cannot be imported or exported from the directory.

### 4.5.4 iPlanet Schema Synchronization Limitations

When synchronizing user data, the iPlanet connector does not synchronize the schema changes automatically. To perform this synchronization, you use `$ORACLE_HOME/bin/schemasync`. The schemasync tool is not supported in the 'SSL' mode.

The SSL mode between the Oracle directory integration server and the iPlanet Directory is not supported in Release 9.0.2.1.0. However, the SSL mode is supported in this release between the Oracle directory integration server and Oracle Internet Directory. Because the Oracle directory integration server can be run from anywhere, it can be co-hosted with the iPlanet Directory.

iPlanet connector comes with a default import and export profiles which are used for synchronization. Before using the iPlanet export connector, you must subscribe to Oracle Internet Directory change events. Otherwise, the change events are purged before they are consumed by the iPlanet connector. To subscribe to change events, the default export profile requires setting the `orclsubscriberdisable` flag to FALSE. By default, this flag is set to TRUE. To set the "`orclsubscriberdisable`" flag to FALSE, use the ldapmodify command-line tool with the LDIF file in `ORACLE_HOME/ldap/odi/conf/iplpurgedisable.ldif`.

### 4.5.5 Limitation in Synchronizing Deletions from iPlanet

If the iPlanet connector is deployed for a two-way synchronization between Oracle Internet Directory and iPlanet Directory Server, then deletion of entries in the iPlanet Directory originally created in Oracle Internet Directory are not propagated to Oracle Internet Directory. Such entries must be deleted in Oracle Internet Directory.

### 4.5.6 Configset0 for Starting Oracle Directory Integration Server Is Reserved For Oracle Provisioning Integration Service

If you use Oracle directory integration server for synchronization—for example, with an iPlanet Directory Server, then use any configset except configset0 when you start the directory integration server. Configset0 is reserved for running Oracle directory integration server for the Oracle Provisioning Integration Service.

### 4.5.7 Data Interface Type DB Not Supported (bug 2193082)

The data interface type, indicating the type of interface used for synchronization between Oracle Internet Directory and connected directory, provides a "DB" option in the user interface. However, selecting that option gives an error message saying that the option is not supported in the directory server. The DB option should not be displayed at all by the user interface.

### 4.5.8 Host Name Attribute Has No Impact on the Execution (bug 2193095)

While configuring a directory integration profile, an attribute `hostname` is shown in Oracle Directory Manager, indicating the host on which the agent is to be run. The value given in that field has no impact on the execution.

### 4.5.9 Migrated Oracle Directory Integration Platform Does Not Launch by Default

In the upgrade process, the Oracle Directory Integration Platform does not come up by default. The Oracle directory integration server needs to be registered and started explicitly after an Oracle Internet Directory upgrade.

### 4.5.10 Uploading Mapping and Configuration Information to Connector Profiles

Use the following arguments with ldapUploadAgentFile.sh for uploading mapping and configuration information for Oracle Directory Integration Platform agents into Oracle Internet Directory connector profile entries:

***Table 1 Arguments for ldapUploadAgentFile.sh***

| Argument | Description |
|---|---|
| `name` | The name of the integration profile to which the information needs to be loaded. |
| `config` | The configset to which the profile belongs to. |
| `LDAPhost` | Directory server host |
| `LDAPport` | Directory server Port |
| `binddn` | Bind DN of the directory user who has access rights to modify the profile entry. |
| `bindpass` | Password corresponding to the bind DN |
| `attrtype` | Type of file to be loaded. "MAP" is specified for loading the mapping file. And "ATTR" is specified for loading the configuration information file. |
| `filename` | Complete path name of the file to be uploaded. |

### 4.5.11 Post-Upgrade Step for iPlanet Synchronization

As part of upgrade, Integration Profiles for iPlanet synchronization, namely iPlanetImport and iPlanetExport are created. For these profiles to be configured and used for synchronization, they need to be added to configset1. If the profiles are available in Configset 1 as part of upgrade, it will be shown in ODM under Integration Server as part of Configuration Set1. If the profiles are not available, they can be added by using LDAPMODIFY as below:

```
ldapmodify -h <OID Host> -p <OID Port> -D <OID Super-user> -w <OID
Super-user @ password> -f <ORACLE_HOME>/ldap/install/upgdip.ldif
```

## 4.6 Directory Server Limitations

### 4.6.1 Oracle Directory Server and Database Tools Can Run on Non-UTF8 Databases

The Oracle directory server and database tools are no longer restricted to run on a UTF8 database. However, if the character set of the data in the client request differs from that in the directory server database, and if that client data cannot be mapped to the database character set, then there may be data loss during LDAP add, delete, modify, or modifydn operations. Oracle Corporation recommends that the client and database character sets be the same if the database underlying the Oracle directory server is not UTF8.

### 4.6.2 If Directory Is Not Populated by Using the bulkload Utility, then OIDSTATS Must Be Run

If bulkload.sh is not used to populate the directory, then `$ORACLE_HOME/ldap/admin/oidstats.sh` must be run. Otherwise, there may be significant search performance degradation. The DBMS_STATS() PL/SQL package may be used instead of oidstats.sh.

### 4.6.3 Installation of Replicated Directories in a Logical Host Environment

Oracle Internet Directory supports failover in a clustered environment by using logical hosts described in "Managing Failover in Clusters" in the *Oracle Internet Directory Administrator's Guide.* Use of logical hosts in a replication environment requires a fresh installation of Oracle Internet Directory. It also requires the use of logical host names while configuring the replication agreement. If you are upgrading from an existing pre-3.0.1 replication environment where host names in the existing replication agreement differ from the logical host names, then replication fails.

### 4.6.4 Transparent Application Failover (TAF) Does Not Work Reliably In Real Application Clusters Configurations

In Oracle Internet Directory Release 9.0.2.1.0, connection-time failover works. Transparent application failover does not always work, but, when it fails, it falls back to connection-time failover.

### 4.6.5 Indexed Attribute Names Cannot Exceed 28 Characters

You cannot use catalog.sh to create an index on an attribute if the attribute has more than 28 characters in its name.

### 4.6.6 Only Attributes With Supported Matching Rules Can Be Indexed

You must assign a matching rule supported by Oracle Internet Directory to any new attribute definition before indexing that attribute. See the *Oracle Internet Directory Administrator's Guide* for more details on using the catalog.sh utility and on supported matching rules and their syntax.

### 4.6.7 Integer Match for Equality of Indexed Attributes Behaves Like a String Match

When an attribute with `integerMatch` for EQUALITY is indexed by using catalog.sh, the matching rule of the attribute works like that of a string rather than that of an integer.

### 4.6.8 Attribute Alias Dereferencing Not Supported in LDAP Operations

Oracle Internet Directory Release 9.0.2.1.0 supports entry alias dereferencing in LDAP operations, but not attribute dereferencing.

### 4.6.9 Syntax Checking Is Not Supported in the Directory Server

The Oracle directory server does not verify the syntax of the attribute values entered by users during entry addition and modification.

### 4.6.10 SSL V2 Clients May Not Be Able to Connect to the Server

LDAP clients using SSL v2 may experience "Can't Contact LDAP server" errors sporadically in attempting to bind to Oracle Internet Directory servers.

### 4.6.11 New SSL Support for Replication Server Connections to the Directory Server

In Oracle Internet Directory Release 9.0.2.1.0, the directory server replication processes can use SSL (Mode 1 - No Authentication) to connect to SSL-based directory server processes. Previous releases of Oracle Internet Directory did not have this capability.

### 4.6.12 Oracle Internet Directory Server Entry Cache Is Automatically Disabled in Multi-Server Instances and in Replication Groups

This is because the greatest entry cache performance improvements are achieved when the "working set " of entries in a deployment are up to a few 100k of entries, and client concurrency of up to a 1000 clients—that is, when the "working set" of entries are completely cached and a single server can handle all the concurrent clients.

### 4.6.13 The OIDCTL/ODISRV SSLAUTH Flag

The OIDCTL command-line tool takes an SSLAUTH argument whenever `server=odisrv` is specified. Contrary to the documentation, the legal values for `sslauth` are 0,1 and 2, corresponding to the meanings in the following table.

***Table 2 Values for SSLAUTH***

| Argument | Meaning |
|---|---|
| 0 | SSL is not used. (Non-SSL mode) |
| 1 | SSL used for encryption only, i.e., with no PKI authentication; a wallet is not used in this case. |
| 2 | SSL is used with one-way authentication—this mode requires you to specify a complete path name of an Oracle Wallet, including the file name itself, unlike other Oracle Internet Directory tools which expect only the wallet location. For example, you would enter something like the following:<br>`oidctl server=odisrv instance=instance_number configset=configset_number flags="host=myhost port=myport sslauth=2 wloc=file:/home/mydir/mywallet.dat wpass=welcome" (server/complete installations)`<br>`odisrv host=myhost port=myport sslauth=2 wloc=file:/home/mydir/mywallet.dat wpass=welcome (client-only installations)`<br>rather than this:<br>`oidctl server=odisrv instance=instance_number configset=configset_number flags="host=myhost port=myport sslauth=2 wloc=file:/home/mydir wpass=welcome" (server/complete installations)`<br>`odisrv host=myhost port=myport sslauth=2 wloc=file:/home/mydir wpass=welcome`<br><br>**Note:** The wallet for the Oracle directory integration server must be a text wallet created using the "Export Wallet" option of the Oracle Wallet Manager. Refer to the Oracle Wallet Manager in the *Oracle Internet Directory Administrator's Guide* for more details on exporting wallets. |

### 4.6.14 Plain Wallets No Longer Supported, Replaced by Local Wallets

With Oracle Internet Directory Release 9.0.2.1.0, use of plain—that is, unencrypted ewallet—wallets is no longer supported, and is replaced by "local" or "encrypted" wallets—that is, cwallet.sso wallets that are encrypted on the file system. Because they are not encrypted, plain wallets require a user name and password to access. Local wallets, which store their own passwords in encrypted form, do not require passwords for their owners to open them.

When the operating system user who created the local wallet opens it, the wallet password is decrypted and used for reading the wallet contents. Only the system user who created a local wallet can open it, as it is stored in a form that is encrypted by using the operating system user name, host name, and other operating system-specific data. For this reason, so that SSL-enabled Oracle Internet Directory listeners can use them for two-way SSL authentication, the same operating system user that owns the Oracle Internet Directory executables must create Oracle Internet Directory server-side wallets specified in the SSL configset (or in the flags passed to OIDCTL and ODISRV). In the Windows operating system, the OID Service should run as the user who created the wallet. By default, the OID Service runs as the local system account.

### 4.6.15 Default Port 389

Chapter 11 of the *Oracle Internet Directory Administrator's Guide* refers to the default port for non-SSL LDAP processes as "839". This should read "389" as is stated elsewhere in the documentation.

### 4.6.16 Password Policy Limitations

Entries under Root Oracle Context are excluded from any password policy.

If a subscriber does not specify its user search base, then the Root Oracle Context password policy applies to all users in the domain of that subscriber. If a user search base in specified by the subscriber, then the password policy under the Subscriber Oracle Context applies to all of its users.

During upgrade from any 9*i* version of Oracle Internet Directory, the existing password policy is moved to the Root Oracle Context.

### 4.6.17 Limitations of Oracle Internet Directory Credential Framework

Oracle Internet Directory password policies do not apply to the Oracle Internet Directory verifier attribute types, namely `authpassword` and `orclpasswordverifier`.

### 4.6.18 Using Oracle Internet Directory with Oracle9*i*AS Portal and Oracle9*i*AS Single Sign-On

When Oracle9*i*AS Portal is installed, a user entry is created under the default user creation base for the default subscriber, `cn=PUBLIC,cn=users,o=mycompany,dc=com`. This entry represents any unauthenticated user, and is required for proper operation of Oracle9*i*AS Portal and Oracle9*i*AS Single Sign-On. This user account should not be removed. If this user entry is missing, it causes significant performance degradation in the directory server because of repeated attempts to locate the entry.

If you are configuring Oracle9*i*AS to use an existing directory information tree (DIT), then be sure that the default user search base includes a user named PUBLIC for this purpose. For a user base of `cn=users,o=oracle,dc=com`, this entry has the following definition:

```
dn: cn=PUBLIC,cn=users,o=oracle,dc=com
cn: PUBLIC
sn: PUBLIC
objectclass: top
objectclass: person
objectclass: inetOrgPerson
objectclass: organizationalPerson
objectclass: orclUser
objectclass: orclUserV2
```

Note the absence of the `userPassword` attribute. No `userPassword` attribute should be provided to disallow logging on as this user through Oracle9*i*AS Single Sign-On.

### 4.6.19 Run New OIDEMDPASSWD Tool Whenever Using OIDPASSWD Tool

Whenever you change the Oracle Internet Directory database user ODS password by using the oidpasswd utility, run the new oidemdpasswd utility. This enables the Oracle Enterprise Manager Daemon (a component of Oracle Enterprise Manager) to properly cache the ODS password. Without this step, you cannot monitor Oracle Internet Directory processes from the Oracle Enterprise Manager. This is because the Oracle Enterprise Manager Daemon component cannot contact the ODS schema upon starting up.

### 4.6.20 Entry Cache Must Be Disabled for Running Bulk Tools

The entry cache must be disabled in order to run any bulk tools. Otherwise results returned for subsequent queries will be incorrect. Bulkmodify and bulkdelete are the tools of interest here.

### 4.6.21 OID Service Does Not Start Automatically at Reboot if Database Is Not Up

On the Windows operating system, it is required that the OID Service start automatically when the computer is rebooted. However, the OID Service requires Oracle database to be running. When the computer is rebooted, the OID Service may not start automatically if the Oracle database is not yet running. After you reboot the computer, be sure that the Oracle database is running, then manually start the OID Service—Oracle*ORACLE_HOME_NAME*InternetDirectory.

### 4.6.22 OID Service User Must Be the Same Oracle Database User

On the Windows operating system, the OID Service—Oracle*ORACLE_HOME_NAME*InternetDirectory—needs to be run as the same user as that of the Oracle database service.

### 4.6.23 Oracle Internet Directory Server May Log Extra Information When LDAP Main Page Is Accessed

When you access the LDAP main page of EMD, the Oracle Internet Directory server may log extra information in a log file named `oidldap00.log`. This log file can be ignored.

### 4.6.24 Updated Information for Oracle Internet Directory Port Numbers

In order to bring up the Oracle Internet Directory server on the default non-SSL port 389 and SSL port 636 at the end of the installation, the following conditions must hold true:

- The default ports 389, 636 should not be in use.
- The `/etc/services` file should not have any line containing these port numbers.

If either of these conditions is not met, the Oracle Internet Directory server will be brought up on a different port which is logged in the file *`ORACLE_HOME`*`/ldap/install/oidca.out`.

## 4.7 Directory Replication Limitations

### 4.7.1 Creating New Directory Replication Groups

The section in the *Oracle Internet Directory Administrator's Guide*about creating new directory replication groups (DRGs) assumes that there is no pre-existing directory data on any of the nodes being used for the DRG.

### 4.7.2 Adding New Nodes to Existing Directory Replication Groups

In Oracle Internet Directory Release 9.0.2.1.0, you cannot create a directory replication group from an existing, non-replicating single Oracle Internet Directory node by using the documented "add a node" procedure. The procedure assumes you have an existing DRG and wish to increase the number of participating nodes by one. In this case, you need to ensure that there is no pre-existing data on the new node. Any pre-existing data is not replicated back to the other participants in the existing DRG. If it is necessary to replicate pre-existing data, then do the following:

1. Extract the data to an LDIF file by using ldapsearch with the -L option.
2. Delete all exported entries from the new node.
3. After the new node is added to the DRG and can replicate new data to the other nodes, reload the exported data by using ldapadd.

### 4.7.3 Do Not Use bulkload.sh to Add Data to a Node That Is Already Part of an Active Replication Agreement

Once a directory server instance is participating in a replication agreement, do not use bulkload.sh to add data into the node. Use ldapadd instead.

### 4.7.4 The Directory Replication Server Does Not Preserve Spaces Between RDN Components

The directory replication server does not always preserve the spaces between RDN components in the DN during entry replication. In some rare cases, it may not preserve the case of the letters in the DN.

### 4.7.5 Local System-Specific Metadata Is Not Replicated

Server configuration, replication agreement, audit log, directory server statistics, event, and DSE root-specific data are not included in the data replicated between servers in a directory replication group.

### 4.7.6 The `cn=Oracle Internet Directory` Container Is Not Replicated

In Release 9.0.2.1.0, the `cn=Oracle Internet Directory` container is not replicated, and therefore change logs associated with any updates under this container will fail at the consumer.

## 4.8 Log File Locations

Oracle Internet Directory components output their log and trace information to log files in the ORACLE_HOME environment. Table 3 lists the components and the locations of the log files for these components.

*Table 3 Components and Their Log File Locations*

| Component | Log File Name |
|---|---|
| LDAP Dispatcher process "oidldapd" | `$ORACLE_HOME/ldap/log/oidldapd`*`XX`*`.log` where *XX* is the server instance number |
| Directory (LDAP) Server process "oidldapd" | `$ORACLE_HOME/ldap/log/oidldapd`*`XX`*`s`*`PID`*`.log` where *PID* is the server process identifier |
| Replication Server process "oidrepld" | `$ORACLE_HOME/ldap/log/oidrepld00.log` |
| Monitor process "oidmon" | `$ORACLE_HOME/ldap/log/oidmon.log` |
| Bulk Loader "bulkload.sh" | `$ORACLE_HOME/ldap/log/install.log` |
| Catalog Manager "catalog.sh" | `$ORACLE_HOME/ldap/log/catalog.log` |
| Replication Setup "ldaprepl.sh" | `$ORACLE_HOME/ldap/admin/logs/ldaprepl.log` |
| Oracle directory integration server process "odisrv" | `$ORACLE_HOME/ldap/log/odisrv`*`XX`*`.log` where *XX* is the OidsyncServer server instance number |
| Directory Integration Profile agent | `$ORACLE_HOME/ldap/odi/log/`*`Agent_Name`*`.err` |

# 5 Oracle Internet Directory Client Release 9.0.2.1.0

The Oracle Internet Directory Client Release 9.0.2.1.0 contains the following software:

- LDAP libraries required by various LDAP clients to communicate with an LDAP server
- Various general purpose LDAP tools such as ldapsearch and ldapadd
- An administrative tool for administering the Oracle directory server
- Oracle Directory Integration Platform

## 5.1 LDAP Tools Limitations

### 5.1.1 LDAPSEARCH Limitations

Approximate matching (or fuzzy matching) of entries is not supported.

### 5.1.2 LDAPSEARCH Does Not Generate LDIF Output by Default

To generate LDIF-formatted output from the ldapsearch command line tool, use the `-L` flag.

### 5.1.3 Catalog Management Tool Usage

The Catalog Index Management tool (catalog.sh) enables you to:

- Convert previously non-searchable attributes into searchable ones by indexing them
- Define and delete indexes on new attributes

Be careful not to use the catalog.sh `-delete` option to remove indexes on attributes unless you are absolutely sure that the indexes were not created by the base schema that was installed with Oracle Internet Directory. Removing indexes from base schema attributes can adversely impact the operation of Oracle Internet Directory. Also see the server side limitations on indexed attributes in Sections 4.6.5 through 4.6.7. You must restart the instances of the Oracle directory server process to recognize the newly cataloged attribute.

### 5.1.4 LDAPADD with -r Option Is Not Supported

Using the ldapadd utility with the `-r` option should replace the entry if there is an entry with the same DN already in the directory. An "object already exists" message is reported when an entry of the same distinguished name already exists in the directory information tree.

## 5.2 Oracle Directory Manager

The Oracle Directory Manager provides an easy to use graphical user interface for administering data and policies in Oracle Internet Directory. It can be launched through command-line invocation (oidadmin).

### 5.2.1 Administering Older Versions of Oracle Internet Directory with Oracle Directory Manager Release 9.0.2.1.0

The version of Oracle Directory Manager shipped with Release 9.0.2.1.0 works with only the following versions of the Oracle Internet Directory server:

- 2.0.4.x
- 2.0.5.x
- 2.0.6.x
- 2.1.1.x
- 3.0.1
- 9.0.2.1.0.

### 5.2.2 Administering Third-Party Directories by Using Oracle Directory Manager

Administering LDAP directories other than Oracle Internet Directory with Oracle Directory Manager is not supported.

### 5.2.3 Oracle Directory Manager Issues and Limitations

**5.2.3.1 Oracle Directory Manager Shows Timestamp Properties Incorrectly for Operational Attributes (Bug 1477787)** All operational timestamp attributes are stored in server as GMT timestamp. But Oracle Directory Manager displays them as local timezone-based.

**5.2.3.2 Oracle Directory Manager Cannot Be Used to Add Object Classes to Existing Entries.** Oracle Internet Directory allows existing entries to be extended—that is, support additional attributes—by adding object classes to their `objectClass` attribute. You cannot perform this form of schema extension by using Oracle Directory Manager. Rather it can be done only by using command-line tools, and must never create schema inconsistencies—for example, an attribute that does not contain a required value. To avoid such inconsistencies, auxiliary object classes with only optional attributes are used exclusively for extending existing entries.

**5.2.3.3 Moving the Scroll Bar on The Help Window Sometimes Crashes the Oracle Directory Manager Session (Bug 2162732)** Oracle Directory Manager online help scrolling can cause the crash of the Java Virtual Machine in a simplified Chinese environment. This problem is seen only on some computers. If you encounter this problem, then replace the contents of the Chinese help to English in the jar file. To achieve this, enter the following commands:

```
cd /tmp
jar xf $ORACLE_HOME/ldap/oidadmin/osdadminhelp.jar
mv -f oracle/ldap/admin/help/ldap/* oracle/ldap/admin/help/ldap_zh_CN/
mv -f  $ORACLE_HOME/ldap/oidadmin/osdadminhelp.jar $ORACLE_
HOME/ldap/oidadmin/osdadminhelp.jar.bak
jar cf $ORACLE_HOME/ldap/oidadmin/osdadminhelp.jar oracle
jar tf $ORACLE_HOME/ldap/oidadmin/osdadminhelp.jar
```

## 5.3 Delegated Administration Issues and Limitations

During "User Delete" confirmation message, the browser refresh gives Null exception (bug 2035381)

To exit Edit User page, you must use the Cancel button (bug 2288441). Otherwise, incorrect user data may be displayed the next time the Edit User page is displayed.

The online help available on the DAS home page is available only in English (bug 2268393).

Uploading JPEG photographs for users fails when there are multibyte characters in the user name (bug 2154745).

Unchecking the enable subscriber logo does not work (bug 2285575).

## 5.4 Oracle Directory Integration Platform Issues and Limitations (Client-Only Installation)

See Section 4.5, "Oracle Directory Integration Platform Issues and Limitations".