

## **Oracle® Fusion Middleware**

Reference for Oracle Identity Management

11g Release 1 (11.1.1)

**E56471-02**

August 2018

Documentation for administrators and developers that provides reference information about the command-line tools and LDAP directory schema elements for Oracle Identity Management.

Oracle Fusion Middleware Reference for Oracle Identity Management 11g Release 1 (11.1.1)

E56471-02

Copyright © 2005, 2018, Oracle and/or its affiliates. All rights reserved.

Primary Author: Devanshi Mohan

Contributing Author: John Spencer

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

---

---

# Contents

<b>Preface</b> .....	xxix
Audience .....	xxix
Documentation Accessibility .....	xxix
Related Documents .....	xxix
Conventions .....	xxx

## Part I Command-Line Tool Reference

### 1 Command-Line Tools Overview

1.1	Using Passwords with Command-Line Tools .....	1-1
1.2	Configuring Your Environment.....	1-2
1.3	Oracle Identity Management Command-Line Tool Categories.....	1-2

### 2 Oracle Internet Directory Administration Tools

2.1	oidpasswd .....	2-1
2.1.1	Syntax for oidpasswd.....	2-2
2.1.2	Arguments for oidpasswd.....	2-2
2.1.3	Tasks and Examples for oidpasswd.....	2-2
2.1.3.1	Changing the Password to the Oracle Internet Directory Database .....	2-3
2.1.3.2	Creating Wallets for Directory Database and Replication Server Passwords .....	2-3
2.1.3.3	Unlocking the Superuser Account .....	2-3
2.1.3.4	Resetting the Superuser Password.....	2-4
2.1.3.5	Managing Superuser Access Control Points .....	2-4
2.1.4	Related Command-Line Tools for oidpasswd.....	2-4
2.2	oidctl .....	2-4
2.2.1	Syntax for oidctl .....	2-5
2.2.2	Arguments for oidctl .....	2-5
2.2.2.1	OIDLDAPD Flags .....	2-6
2.2.2.2	OIDREPLD Flags .....	2-7
2.2.3	Tasks and Examples for oidctl .....	2-7
2.2.3.1	Creating an Oracle Internet Directory Instance in an Existing Component .....	2-8
2.2.3.2	Deleting an Oracle Internet Directory Instance in a Component .....	2-8
2.2.3.3	Starting an Oracle Internet Directory Server Instance .....	2-8
2.2.3.4	Stopping an Oracle Internet Directory Server Instance .....	2-8
2.2.3.5	Restarting an Oracle Internet Directory Server Instance .....	2-9

2.2.3.6	Starting a Directory Replication Server Instance .....	2-9
2.2.3.7	Stopping a Directory Replication Server Instance .....	2-9
2.2.3.8	Starting and Stopping a Server Instance on a Virtual Host or Cluster Node .....	2-9
2.2.3.9	Reporting the Status of Each Server.....	2-10
2.2.3.10	Reporting Diagnostics.....	2-10
2.2.3.11	Reporting Server Manageability Information .....	2-11
2.2.4	Related Command-Line Tools for oidctl.....	2-11
2.3	oiddiag.....	2-11
2.3.1	Syntax for oiddiag.....	2-12
2.3.2	Arguments for oiddiag .....	2-12
2.3.3	Tasks and Examples for oiddiag.....	2-13
2.3.3.1	Collecting All Diagnostic Information .....	2-13
2.3.3.2	Collecting Selected Diagnostic Information .....	2-13
2.3.3.3	Collecting Stack Trace Information.....	2-14
2.4	oidmon.....	2-14
2.4.1	Syntax for oidmon .....	2-14
2.4.2	Arguments for oidmon .....	2-14
2.4.3	Tasks and Examples for oidmon .....	2-15
2.4.3.1	Starting Oracle Internet Directory Monitor .....	2-15
2.4.3.2	Starting Oracle Internet Directory Monitor on a Virtual Host or Cluster Node .....	2-15
2.4.3.3	Stopping Oracle Internet Directory Monitor .....	2-15
2.4.4	Related Command-Line Tools for oidmon .....	2-15
2.5	opmnctl.....	2-15
2.5.1	Syntax for opmnctl .....	2-16
2.5.2	Arguments for opmnctl .....	2-16
2.5.2.1	Commands.....	2-17
2.5.2.2	WebLogic Administration Server Properties .....	2-17
2.5.2.3	Instance Properties .....	2-18
2.5.2.4	OPMN Configuration Properties .....	2-18
2.5.2.5	Component Properties for Oracle Internet Directory .....	2-18
2.5.2.6	Oracle Internet Directory Component Configuration Properties .....	2-18
2.5.3	Tasks and Examples for opmnctl .....	2-19
2.5.3.1	Creating an Oracle Internet Directory Component.....	2-20
2.5.3.2	Registering an Oracle Instance .....	2-20
2.5.3.3	Unregistering an Oracle Instance .....	2-20
2.5.3.4	Updating the Component Registration of an Oracle Instance .....	2-20
2.5.3.5	Deleting an Oracle Internet Directory Component .....	2-21
2.5.3.6	Stopping All Oracle Internet Directory Server Components .....	2-21
2.5.3.7	Starting All Oracle Internet Directory Server Components .....	2-21
2.5.3.8	Stopping a Specific Oracle Internet Directory Server Component .....	2-21
2.5.3.9	Starting a Specific Oracle Internet Directory Server Component .....	2-21
2.5.3.10	Restarting All Oracle Internet Directory Server Components .....	2-21
2.5.3.11	Restarting a Specific Oracle Internet Directory Server Component .....	2-22
2.5.3.12	Getting Status Information.....	2-22
2.5.4	Related Command-Line Tools for opmnctl .....	2-22
2.6	oidstats.sql.....	2-22
2.6.1	Syntax for oidstats.sql .....	2-23

2.6.2	Arguments for oidstats.sql .....	2-23
2.6.3	Tasks and Examples for oidstats.sql .....	2-23
2.6.3.1	Running the Oracle Internet Directory Database Statistics Collection Tool .....	2-23
2.6.4	Related Command-Line Tools for oidstats.sql .....	2-23
2.7	oidcred .....	2-23
2.7.1	Syntax for oidcred.....	2-23
2.7.2	Arguments for oidcred.....	2-23
2.7.3	Tasks and Examples for oidcred.....	2-24
2.8	oidrealm.....	2-24
2.8.1	Syntax for oidrealm .....	2-24
2.8.2	Arguments for oidrealm .....	2-24
2.8.3	Example for oidrealm.....	2-25

### 3 Oracle Internet Directory Data Management Tools

3.1	bulkdelete.....	3-2
3.1.1	Syntax for bulkdelete.....	3-2
3.1.2	Arguments for bulkdelete .....	3-2
3.1.3	Tasks and Examples for bulkdelete .....	3-3
3.1.3.1	Deleting All Entries in a Naming Context and Making Them Tombstone Entries ....	3-3
3.1.3.2	Completely Deleting All Entries in a Naming Context .....	3-3
3.1.3.3	Deleting Entries in Multiple Naming Contexts.....	3-3
3.1.4	Related Command-Line Tools for bulkdelete .....	3-3
3.2	bulkload.....	3-4
3.2.1	Syntax for bulkload .....	3-6
3.2.2	Arguments for bulkload .....	3-6
3.2.3	Tasks and Examples for bulkload .....	3-7
3.2.3.1	Loading Data in Bulk Mode.....	3-8
3.2.3.2	Loading Data for Multiple Nodes in a Replicated Environment .....	3-8
3.2.3.3	Loading Data in Incremental Mode.....	3-8
3.2.3.4	Verifying Indexes.....	3-8
3.2.3.5	Recreating Indexes.....	3-9
3.2.3.6	Recovering Data After a Load Error .....	3-9
3.2.4	Related Command-Line Tools for bulkload .....	3-9
3.3	bulkmodify.....	3-9
3.3.1	Syntax for bulkmodify .....	3-10
3.3.2	Arguments for bulkmodify .....	3-10
3.3.3	Tasks and Examples for bulkmodify .....	3-11
3.3.3.1	Updating an Attribute for Multiple Entries at Once .....	3-11
3.3.4	Limitations of bulkmodify.....	3-12
3.3.5	Related Command-Line Tools for bulkmodify .....	3-12
3.4	catalog.....	3-12
3.4.1	Syntax for catalog.....	3-13
3.4.2	Arguments for catalog .....	3-13
3.4.3	Tasks and Examples for catalog .....	3-14
3.4.3.1	Indexing a Single Attribute .....	3-14
3.4.3.2	Indexing Multiple Attributes.....	3-14

3.4.3.3	Removing an Attribute from the List of Indexed Attributes .....	3-14
3.4.3.4	Indexing an Attribute Using the IOT Option .....	3-15
3.4.4	Related Command-Line Tools for catalog .....	3-15
3.5	ldapadd.....	3-15
3.5.1	Syntax for ldapadd .....	3-15
3.5.2	Arguments for ldapadd .....	3-15
3.5.3	Tasks and Examples for ldapadd .....	3-18
3.5.3.1	Adding Data to the Directory Using an LDIF File.....	3-18
3.5.3.2	Adding Data to the Directory Using a DSML File .....	3-18
3.5.3.3	Previewing an Add Operation .....	3-19
3.5.4	Related Command-Line Tools for ldapadd .....	3-19
3.6	ldapaddmt.....	3-19
3.6.1	Syntax for ldapaddmt .....	3-19
3.6.2	Arguments for ldapaddmt .....	3-19
3.6.3	Tasks and Examples for ldapaddmt .....	3-22
3.6.3.1	Adding Concurrent Entries to the Directory Using an LDIF File .....	3-22
3.6.4	Related Command-Line Tools for ldapaddmt .....	3-22
3.7	ldapbind .....	3-22
3.7.1	Syntax for ldapbind .....	3-22
3.7.2	Arguments for ldapbind.....	3-22
3.7.3	Tasks and Examples for ldapbind .....	3-24
3.7.3.1	Validating Authentication Credentials .....	3-24
3.7.4	Related Command-Line Tools for ldapbind.....	3-24
3.8	ldapcompare .....	3-24
3.8.1	Syntax for ldapcompare.....	3-24
3.8.2	Arguments for ldapcompare.....	3-24
3.8.3	Tasks and Examples for ldapcompare.....	3-26
3.8.3.1	Comparing Attribute Values for an Entry .....	3-27
3.8.4	Related Command-Line Tools for ldapcompare.....	3-27
3.9	ldapdelete.....	3-27
3.9.1	Syntax for ldapdelete.....	3-27
3.9.2	Arguments for ldapdelete .....	3-27
3.9.3	Tasks and Examples for ldapdelete .....	3-29
3.9.3.1	Deleting a Single Entry .....	3-29
3.9.3.2	Deleting Multiple Entries Using an LDIF File.....	3-29
3.9.4	Related Command-Line Tools for ldapdelete .....	3-29
3.10	ldapmoddn.....	3-29
3.10.1	Syntax for ldapmoddn .....	3-30
3.10.2	Arguments for ldapmoddn .....	3-30
3.10.3	Tasks and Examples for ldapmoddn .....	3-31
3.10.3.1	Changing the RDN of an Entry .....	3-32
3.10.3.2	Moving an Entry.....	3-32
3.10.4	Related Command-Line Tools for ldapmoddn .....	3-32
3.11	ldapmodify.....	3-32
3.11.1	Syntax for ldapmodify .....	3-32
3.11.2	Arguments for ldapmodify .....	3-32
3.11.3	Tasks and Examples for ldapmodify .....	3-35

3.11.3.1	Modifying the Directory Schema .....	3-35
3.11.3.2	Modifying an Entry .....	3-36
3.11.3.3	Indexing an Attribute.....	3-36
3.11.4	Related Command-Line Tools for ldapmodify .....	3-36
3.12	ldapmodifymt.....	3-36
3.12.1	Syntax for ldapmodifymt .....	3-37
3.12.2	Arguments for ldapmodifymt .....	3-37
3.12.3	Tasks and Examples for ldapmodifymt .....	3-39
3.12.3.1	Modifying Multiple Entries Concurrently.....	3-39
3.12.4	Related Command-Line Tools for ldapmodifymt .....	3-40
3.13	ldapsearch .....	3-40
3.13.1	Syntax for ldapsearch.....	3-40
3.13.2	Arguments for ldapsearch.....	3-40
3.13.3	Tasks and Examples for ldapsearch.....	3-45
3.13.3.1	Performing a Base Object Search.....	3-45
3.13.3.2	Performing a One-Level Search.....	3-45
3.13.3.3	Performing a Subtree Search.....	3-45
3.13.3.4	Searching for Attribute Values of Entries .....	3-45
3.13.3.5	Searching for Operational Attributes of Entries .....	3-46
3.13.3.6	Searching for Entries with Attribute Options .....	3-46
3.13.3.7	Searching for All User Attributes and Specified Operational Attributes.....	3-46
3.13.3.8	Searching for Entries (More Examples).....	3-47
3.13.3.9	Attribute Case in ldapsearch Output.....	3-47
3.13.4	Related Command-Line Tools for ldapsearch.....	3-48
3.14	ldifmigrator.....	3-48
3.14.1	Syntax for ldifmigrator.....	3-48
3.14.2	Arguments for ldifmigrator .....	3-48
3.14.3	Tasks and Examples for ldifmigrator .....	3-49
3.14.3.1	Using the Data Migration Tool in Lookup Mode .....	3-50
3.14.3.2	Overriding Data Migration Values in Lookup Mode .....	3-50
3.14.3.3	Using the Data Migration Tool by Supplying Your Own Values .....	3-50
3.14.3.4	Loading and Reconciling Data Using the Data Migration Tool .....	3-50
3.14.4	Related Command-Line Tools for ldifmigrator .....	3-50
3.14.5	Error Messages for ldifmigrator .....	3-50
3.15	ldifwrite .....	3-52
3.15.1	Syntax for ldifwrite.....	3-52
3.15.2	Arguments for ldifwrite.....	3-53
3.15.3	Tasks and Examples for ldifwrite.....	3-53
3.15.3.1	Converting All Entries under a Naming Context to an LDIF File.....	3-53
3.15.3.2	Converting a Partial Naming Context to an LDIF File .....	3-54
3.15.3.3	Converting Entries that Match Criteria to an LDIF File .....	3-54
3.15.4	Related Command-Line Tools for ldifwrite.....	3-54
3.16	upgradecert.pl .....	3-54
3.16.1	Syntax for upgradecert.pl.....	3-55
3.16.2	Arguments for upgradecert.pl.....	3-55
3.16.3	Tasks and Examples for upgradecert.pl.....	3-55

3.16.3.1	Upgrading User Certificates Stored in the Directory from Releases Prior to 10.1.2...	3-56
3.16.4	Related Command-Line Tools for upgradecert.pl.....	3-56

## 4 Oracle Internet Directory Replication Management Tools

4.1	ManageHiq.retry and ManageHiq.purge.....	4-1
4.1.1	Syntax for ManageHiq.retry and ManageHiq.purge .....	4-2
4.1.2	Examples for ManageHiq.retry .....	4-2
4.1.3	Examples for ManageHiq.purge .....	4-2
4.2	oidcmprec.....	4-3
4.2.1	Syntax for oidcmprec .....	4-3
4.2.2	Arguments for oidcmprec .....	4-5
4.2.3	Tasks and Examples for oidcmprec .....	4-18
4.2.3.1	Comparing and Reconciling Individual Entries in Two Directories .....	4-18
4.2.3.2	Comparing and Reconciling Subtrees in Two Directories .....	4-18
4.2.3.3	Comparing and Reconciling Entire Directories .....	4-19
4.2.3.4	Performing User-Defined Compare and Reconcile Operations .....	4-20
4.2.3.5	Merging Two Directories.....	4-20
4.2.3.6	Including and Excluding Attributes .....	4-20
4.2.3.7	Using a Filter .....	4-21
4.2.3.8	Overriding Default Conflict Resolution Rules .....	4-21
4.2.3.9	Using a Parameter File.....	4-21
4.2.3.10	Using a Parameter File in XML Format.....	4-22
4.2.3.11	Generating Change Logs .....	4-23
4.2.3.12	Performing Directory Schema Operations.....	4-23
4.3	remtool.....	4-24
4.3.1	Syntax for remtool .....	4-24
4.3.2	Terminology Used in remtool Argument Descriptions .....	4-24
4.3.3	Arguments for remtool .....	4-25
4.3.4	The remtool -asr2ldap Operation .....	4-27
4.3.4.1	Syntax for remtool -asr2ldap.....	4-27
4.3.4.2	Arguments for remtool -asr2ldap .....	4-27
4.3.4.3	Tasks and Examples for remtool -asr2ldap .....	4-27
4.3.4.3.1	Converting an Advanced Replication Agreement to an LDAP-Based Agreement .....	4-27
4.3.5	The remtool -addnode Operation.....	4-28
4.3.5.1	Syntax for remtool -addnode .....	4-28
4.3.5.2	Arguments for remtool -addnode.....	4-28
4.3.5.3	Tasks and Examples for remtool -addnode.....	4-28
4.3.5.3.1	Adding a New Node to an Oracle Database Advanced Replication-based DRG .....	4-28
4.3.6	The remtool -asrcleanup Operation .....	4-30
4.3.6.1	Syntax for remtool -asrcleanup.....	4-30
4.3.6.2	Arguments for remtool -asrcleanup .....	4-30
4.3.6.3	Tasks and Examples for remtool -asrcleanup .....	4-31
4.3.6.3.1	Cleaning Up an Oracle Database Advanced Replication-based DRG Setup .....	4-31
4.3.7	The remtool -asrrectify Operation.....	4-32



4.3.7.1	Syntax for remtool -asrrectify .....	4-32
4.3.7.2	Arguments for remtool -asrrectify .....	4-32
4.3.7.3	Tasks and Examples for remtool -asrrectify .....	4-32
4.3.7.3.1	Detecting and Correcting Errors in an Advanced Replication-Based DRG Setup .....	4-32
4.3.8	The remtool -asrsetup Operation .....	4-33
4.3.8.1	Syntax for remtool -asrsetup .....	4-34
4.3.8.2	Arguments for remtool -asrsetup .....	4-34
4.3.8.3	Tasks and Examples for remtool -asrsetup .....	4-34
4.3.8.3.1	Creating an Oracle Database Advanced Replication-based DRG .....	4-34
4.3.9	The remtool -asrverify Operation .....	4-36
4.3.9.1	Syntax for remtool -asrverify .....	4-37
4.3.9.2	Arguments for remtool -asrverify .....	4-37
4.3.9.3	Tasks and Examples for remtool -asrverify .....	4-37
4.3.9.3.1	Detecting Errors in an Oracle Database Advanced Replication-Based DRG Setup .....	4-37
4.3.10	The remtool -backupmetadata Operation .....	4-38
4.3.10.1	Syntax for remtool -backupmetadata .....	4-38
4.3.10.2	Arguments for remtool -backupmetadata .....	4-39
4.3.10.3	Tasks and Examples for remtool -backupmetadata .....	4-39
4.3.10.3.1	Adding the Metadata of a Pilot Replica to a Master Replica .....	4-39
4.3.10.3.2	Backing Up the Metadata of a Pilot Replica to an LDIF File .....	4-40
4.3.11	The remtool -chgpwd Operation .....	4-40
4.3.11.1	Syntax for remtool -chgpwd .....	4-40
4.3.11.2	Arguments for remtool -chgpwd .....	4-40
4.3.11.3	Tasks and Examples for remtool -chgpwd .....	4-40
4.3.11.3.1	Changing the Administrator Password for an Advanced Replication-based DRG .....	4-40
4.3.12	The remtool -delnode Operation .....	4-41
4.3.12.1	Syntax for remtool -delnode .....	4-41
4.3.12.2	Arguments for remtool -delnode .....	4-42
4.3.12.3	Tasks and Examples for remtool -delnode .....	4-42
4.3.12.3.1	Removing a RMS Node from an Advanced Replication-Based DRG .....	4-42
4.3.13	The remtool -dispasrerr Operation .....	4-43
4.3.13.1	Syntax for remtool -dispasrerr .....	4-43
4.3.13.2	Arguments for remtool -dispasrerr .....	4-43
4.3.13.3	Tasks and Examples for remtool -dispasrerr .....	4-43
4.3.13.3.1	Displaying Errors for an Oracle Database Advanced Replication-based DRG ..	4-44
4.3.14	The remtool -dispqstat Operation .....	4-44
4.3.14.1	Syntax for remtool -dispqstat .....	4-44
4.3.14.2	Arguments for remtool -dispqstat .....	4-45
4.3.14.3	Tasks and Examples for remtool -dispqstat .....	4-45
4.3.14.3.1	Displaying Queue Statistics for an Advanced Replication-Based DRG .....	4-45
4.3.15	The remtool -paddnode Operation .....	4-46
4.3.15.1	Syntax for remtool -paddnode .....	4-46
4.3.15.2	Arguments for remtool -paddnode .....	4-46
4.3.15.3	Tasks and Examples for remtool -paddnode .....	4-46

4.3.15.3.1	Adding a Read-Only Replica to a DRG.....	4-46
4.3.15.3.2	Adding a Partial Replica to a DRG .....	4-48
4.3.16	The remtool -pdisplay Operation.....	4-50
4.3.16.1	Arguments to remtool -pdisplay.....	4-50
4.3.17	The remtool -pchgmaster Operation.....	4-50
4.3.17.1	Syntax for remtool -pchgmaster .....	4-50
4.3.17.2	Arguments for remtool -pchgmaster .....	4-50
4.3.17.3	Tasks and Examples for remtool -pchgmaster .....	4-51
4.3.17.3.1	Breaking a Supplier Agreement and Creating a New One for a Consumer .....	4-51
4.3.17.3.2	Changing the Primary Node.....	4-52
4.3.18	The remtool -pchgpwd Operation .....	4-53
4.3.18.1	Syntax for remtool -pchgpwd.....	4-53
4.3.18.2	Arguments for remtool -pchgpwd.....	4-53
4.3.18.3	Tasks and Examples for remtool -pchgpwd.....	4-53
4.3.18.3.1	Changing the Replication DN Password Used for LDAP-Based Replication.....	4-53
4.3.19	The remtool -pchgwalpwd Operation.....	4-54
4.3.19.1	Syntax for remtool -pchgwalpwd .....	4-54
4.3.19.2	Arguments for remtool -pchgwalpwd .....	4-54
4.3.19.3	Tasks and Examples for remtool -pchgwalpwd .....	4-54
4.3.19.3.1	Changing the Replication DN Password in the Oracle Internet Directory Wallet .....	4-54
4.3.20	The remtool -pcleanup Operation.....	4-55
4.3.20.1	Syntax for remtool -pcleanup .....	4-55
4.3.20.2	Arguments for remtool -pcleanup .....	4-55
4.3.20.3	Tasks and Examples for remtool -pcleanup .....	4-55
4.3.20.3.1	Cleaning Up an Incomplete or Flawed LDAP-based DRG Setup.....	4-55
4.3.20.3.2	Cleaning Up Specific LDAP Agreements .....	4-56
4.3.21	The remtool -pdelnode Operation.....	4-57
4.3.21.1	Syntax for remtool -pdelnode.....	4-57
4.3.21.2	Arguments for remtool -pdelnode.....	4-57
4.3.21.3	Tasks and Examples for remtool -pdelnode.....	4-57
4.3.21.3.1	Deleting a Read-Only Replica from a DRG .....	4-57
4.3.22	The remtool -pdispqstat Operation.....	4-58
4.3.22.1	Syntax for remtool -pdispqstat.....	4-59
4.3.22.2	Arguments for remtool -pdispqstat.....	4-59
4.3.22.3	Tasks and Examples for remtool -pdispqstat.....	4-59
4.3.22.3.1	Display queue statistics for LDAP-based replicas.....	4-59
4.3.23	The remtool -pilotreplica Operation .....	4-59
4.3.23.1	Syntax for remtool -pilotreplica.....	4-59
4.3.23.2	Arguments for remtool -pilotreplica .....	4-60
4.3.23.3	Tasks and Examples for remtool -pilotreplica.....	4-60
4.3.23.3.1	Beginning Pilot Mode for a Replica .....	4-60
4.3.23.3.2	Ending Pilot Mode for a Replica .....	4-60
4.3.24	The remtool -presetpwd Operation .....	4-60
4.3.24.1	Syntax for remtool -presetpwd.....	4-60
4.3.24.2	Arguments for remtool -presetpwd.....	4-60

4.3.24.3	Tasks and Examples for remtool -presetpwd.....	4-61
4.3.24.3.1	Resetting the Replication DN Password for a Single Directory .....	4-61
4.3.25	The remtool -pthput Operation .....	4-61
4.3.25.1	Syntax for remtool -pthput.....	4-61
4.3.25.2	Arguments for remtool -pthput.....	4-61
4.3.25.3	Tasks and Examples for remtool -pthput.....	4-62
4.3.25.3.1	Listing DRG Information at Intervals.....	4-62
4.3.26	The remtool -pverify Operation.....	4-62
4.3.26.1	Syntax for remtool -pverify .....	4-63
4.3.26.2	Arguments for remtool -pverify.....	4-63
4.3.26.3	Tasks and Examples for remtool -pverify.....	4-63
4.3.26.3.1	Verify Replication Configuration for an LDAP-Based DRG.....	4-63
4.3.27	The remtool -resumeasr Operation .....	4-65
4.3.27.1	Syntax for remtool -resumeasr .....	4-65
4.3.27.2	Arguments for remtool -resumeasr .....	4-65
4.3.27.3	Tasks and Examples for remtool -resumeasr .....	4-65
4.3.27.3.1	Resuming Replication Activity for an Advanced Replication-Based DRG	4-66
4.3.28	The remtool -suspendasr Operation .....	4-66
4.3.28.1	Syntax for remtool -suspendasr.....	4-66
4.3.28.2	Arguments for remtool -suspendasr.....	4-66
4.3.28.3	Tasks and Examples for remtool -suspendasr.....	4-66
4.3.28.3.1	Suspending Replication Activity for an Advanced Replication-Based DRG .....	4-67
4.3.29	The -psuspendrepl and -presumerepl Operations.....	4-67
4.3.29.1	Syntax for -psuspendrepl and -presumerepl.....	4-67
4.3.29.2	Arguments to -psuspendrepl and -presumerepl .....	4-67
4.3.29.3	Tasks for -psuspendrepl and -presumerepl.....	4-68
4.3.30	The -bind Connection Argument .....	4-68
4.3.31	The -connect Connection Argument.....	4-68
4.3.32	Related Command-Line Tools for remtool .....	4-69

## 5 Oracle Directory Integration Platform Tools

5.1	manageDIPServerConfig .....	5-1
5.1.1	Syntax for manageDIPServerConfig .....	5-1
5.1.2	Arguments for manageDIPServerConfig.....	5-2
5.1.3	Tasks and Examples for manageDIPServerConfig.....	5-3
5.2	manageSyncProfiles.....	5-3
5.2.1	Syntax for manageSyncProfiles .....	5-3
5.2.2	Arguments for manageSyncProfiles .....	5-4
5.2.3	Tasks and Examples for manageSyncProfiles .....	5-7
5.3	syncProfileBootstrap.....	5-8
5.3.1	Syntax for syncProfileBootstrap .....	5-8
5.3.2	Arguments for syncProfileBootstrap .....	5-8
5.3.3	Tasks and Examples for syncProfileBootstrap .....	5-9
5.4	expressSyncSetup.....	5-10
5.4.1	Syntax for expressSyncSetup .....	5-10
5.4.2	Arguments for expressSyncSetup .....	5-10

5.4.3	Tasks and Examples for expressSyncSetup .....	5-11
5.5	provProfileBulkProv .....	5-12
5.5.1	Syntax for provProfileBulkProv .....	5-12
5.5.2	Arguments for provProfileBulkProv .....	5-12
5.5.3	Tasks and Examples for provProfileBulkProv .....	5-13
5.6	oidprovtool .....	5-13
5.6.1	Syntax for oidprovtool .....	5-14
5.6.2	Arguments for oidprovtool .....	5-14
5.6.3	Tasks and Examples for oidprovtool .....	5-18
5.6.3.1	Creating a Provisioning Profile .....	5-18
5.6.3.2	Modifying a Provisioning Profile .....	5-19
5.6.3.3	Deleting a Provisioning Profile .....	5-19
5.6.3.4	Disabling a Provisioning Profile .....	5-19
5.7	dipStatus .....	5-19
5.7.1	Syntax for dipStatus .....	5-19
5.7.2	Arguments for dipStatus .....	5-20
5.7.3	Examples for dipStatus .....	5-20
5.8	schemasync .....	5-21
5.8.1	Syntax for schemasync .....	5-21
5.8.2	Arguments for schemasync .....	5-21
5.8.3	Tasks and Examples for schemasync .....	5-22
5.8.3.1	Synchronizing the Schema between Oracle Internet Directory and a Third-Party Directory .....	5-22
5.8.4	Related Command-Line Tools for schemasync .....	5-22

## Part II Schema Reference

### 6 LDAP Schema Overview

6.1	Overview of Directory Schema .....	6-1
6.1.1	Object Classes .....	6-1
6.1.2	Attributes .....	6-2
6.1.3	LDAP Controls .....	6-6
6.2	Overview of Oracle Identity Management Schema Elements .....	6-14
6.2.1	System Operational Schema Elements .....	6-15
6.2.1.1	Directory Schema .....	6-15
6.2.1.2	Access Control .....	6-15
6.2.1.3	Change Logs .....	6-15
6.2.1.4	Password Policy .....	6-15
6.2.2	Oracle Internet Directory Configuration Schema Elements .....	6-16
6.2.2.1	Oracle Internet Directory Server .....	6-16
6.2.2.2	Oracle Context .....	6-16
6.2.2.3	Oracle Network Services .....	6-17
6.2.2.4	Garbage Collection .....	6-17
6.2.2.5	Attribute Uniqueness .....	6-17
6.2.3	Audit and Error Logging Schema Elements .....	6-17
6.2.4	Server Manageability Schema Elements .....	6-18
6.2.5	Oracle Directory Replication Schema Elements .....	6-18

6.2.6	Oracle Directory Integration and Provisioning Schema Elements.....	6-19
6.2.6.1	Applications .....	6-19
6.2.6.2	Change Logs.....	6-19
6.2.6.3	Events and Objects .....	6-19
6.2.6.4	Plug-ins and Interfaces .....	6-20
6.2.6.5	Server Configuration.....	6-20
6.2.6.6	Profiles.....	6-20
6.2.6.7	Schema .....	6-21
6.2.6.8	Active Directory Users.....	6-21
6.2.7	Oracle Delegated Administration Services Schema Elements .....	6-21
6.2.8	Oracle Application Server Certificate Authority and PKI Schema Elements .....	6-22
6.2.9	Application Schema Elements .....	6-22
6.2.10	Resource Schema Elements .....	6-22
6.2.11	Plug-in Schema Elements .....	6-22
6.2.12	Directory User Agents Schema Elements.....	6-23
6.2.13	User, Group, and Subscriber Schema Elements.....	6-23
6.2.13.1	Groups.....	6-23
6.2.13.2	Dynamic Groups.....	6-23
6.2.13.3	Users .....	6-24
6.2.14	Password Policy Schema Elements .....	6-24
6.2.15	Password Verifier Schema Elements .....	6-24

## 7 LDAP Object Class Reference

7.1	Standard LDAP Object Classes.....	7-1
7.2	Oracle Identity Management Object Class Reference.....	7-3
7.2.1	duaConfigProfile.....	7-3
7.2.2	orclADGroup.....	7-4
7.2.3	orclADUser .....	7-4
7.2.4	orclApplicationEntity.....	7-4
7.2.5	orclAppSpecificUserInfo.....	7-5
7.2.6	orclAppUserEntry .....	7-5
7.2.7	orclAuditOC .....	7-6
7.2.8	orclCertIdMapping.....	7-6
7.2.9	orclChangeSubscriber .....	7-7
7.2.10	orclCommonAttributes .....	7-7
7.2.11	orclCommonAttributesV2 .....	7-8
7.2.12	orclConfigSet .....	7-8
7.2.13	orclContainer .....	7-8
7.2.14	orclDASAppContainer.....	7-9
7.2.15	orclDASAttrCategory.....	7-9
7.2.16	orclDASConfigAttr.....	7-10
7.2.17	orclDASConfigPublicGroup .....	7-10
7.2.18	orclDASLOVVal.....	7-10
7.2.19	orclDASOperationURL.....	7-11
7.2.20	orclDASSubscriberContainer .....	7-11
7.2.21	orclIDMapping.....	7-12
7.2.22	orclDSAConfig .....	7-12

7.2.23	orclDynamicGroup .....	7-13
7.2.24	orclDynamicList .....	7-13
7.2.25	orclEventLog .....	7-14
7.2.26	orclEvents .....	7-14
7.2.27	orclGeneralStats .....	7-14
7.2.28	orclGroup .....	7-15
7.2.29	orclHealthStats .....	7-15
7.2.30	orclIndexOC .....	7-16
7.2.31	orclLDAPInstance .....	7-16
7.2.32	orclLDAPSubConfig .....	7-17
7.2.33	orclNTUser .....	7-17
7.2.34	orclODIPApplicationCommonConfig .....	7-17
7.2.35	orclODIPAppSubscription .....	7-18
7.2.36	orclODIPEventContainer .....	7-18
7.2.37	orclODIPIntegrationProfile .....	7-19
7.2.38	orclODIPObject .....	7-19
7.2.39	orclODIPPlugin .....	7-20
7.2.40	orclODIPPluginContainer .....	7-20
7.2.41	orclODIPProvEventDefn .....	7-21
7.2.42	orclODIPProvEventTypeConfig .....	7-21
7.2.43	orclODIPProvInterfaceDetails .....	7-21
7.2.44	orclODIPProvisioningIntegrationInBoundProfileV2 .....	7-22
7.2.45	orclODIPProvisioningIntegrationOutBoundProfile .....	7-22
7.2.46	orclODIPProvisioningIntegrationOutBoundProfileV2 .....	7-23
7.2.47	orclODIPProvisioningIntegrationProfile .....	7-23
7.2.48	orclODIPProvisioningIntegrationProfileV2 .....	7-24
7.2.49	orclODIPProfile .....	7-24
7.2.50	orclODIPSchemaDetails .....	7-25
7.2.51	orclODIPServerConfig .....	7-25
7.2.52	orclODISConfig .....	7-26
7.2.53	orclODIServer .....	7-26
7.2.54	orclODISInstance .....	7-27
7.2.55	orclPerfStats .....	7-27
7.2.56	orclPKICRL .....	7-28
7.2.57	orclPKIVaMecCl .....	7-28
7.2.58	orclPluginConfig .....	7-28
7.2.59	orclPluginContainer .....	7-29
7.2.60	orclPluginUser .....	7-29
7.2.61	orclPurgeConfig .....	7-30
7.2.62	orclPwdVerifierPolicy .....	7-30
7.2.63	orclPwdVerifierProfile .....	7-31
7.2.64	orclReplAgreementEntry .....	7-31
7.2.65	orclReplicaSubentry .....	7-31
7.2.66	orclReplInstance .....	7-32
7.2.67	orclReplNameCtxConfig .....	7-32
7.2.68	orclReplSubConfig .....	7-33
7.2.69	orclResourceDescriptor .....	7-33

7.2.70	orclResourceType .....	7-34
7.2.71	orclRootContext .....	7-34
7.2.72	orclSchemaVersion .....	7-34
7.2.73	orclSecRefreshEvents .....	7-35
7.2.74	orclService .....	7-35
7.2.75	orclServiceInstance .....	7-36
7.2.76	orclServiceInstanceReference .....	7-36
7.2.77	orclServiceRecipient .....	7-37
7.2.78	orclServiceSubscriptionDetail .....	7-37
7.2.79	orclServiceSuite .....	7-37
7.2.80	orclSM .....	7-38
7.2.81	orclSubscriber .....	7-38
7.2.82	orclSysResourceEvents .....	7-39
7.2.83	orclTraceConfig .....	7-39
7.2.84	orclUniqueConfig .....	7-40
7.2.85	orclUserStats .....	7-40
7.2.86	orclUserV2 .....	7-41
7.2.87	pwdpolicy .....	7-41
7.2.88	subentry .....	7-42
7.2.89	subregistry .....	7-42
7.2.90	subschema .....	7-42
7.2.91	tombstone .....	7-43
7.2.92	top .....	7-43

## 8 LDAP Attribute Reference

8.1	Standard LDAP Attributes .....	8-1
8.2	Oracle Identity Management Attribute Reference .....	8-5
8.2.1	attributeMap .....	8-5
8.2.2	attributeTypes .....	8-6
8.2.3	authenticationMethod .....	8-6
8.2.4	authPassword .....	8-6
8.2.5	bindAuthPriv .....	8-7
8.2.6	bindTimeLimit .....	8-7
8.2.7	c .....	8-8
8.2.8	changeloginfo .....	8-8
8.2.9	changestatus .....	8-8
8.2.10	cn .....	8-9
8.2.11	contentRules .....	8-9
8.2.12	createTimestamp .....	8-10
8.2.13	creatorsName .....	8-10
8.2.14	credentialLevel .....	8-10
8.2.15	defaultSearchBase .....	8-11
8.2.16	defaultSearchScope .....	8-11
8.2.17	defaultServerList .....	8-11
8.2.18	description .....	8-12
8.2.19	displayName .....	8-12
8.2.20	followReferrals .....	8-13

8.2.21	javaClassName .....	8-13
8.2.22	jpegPhoto .....	8-13
8.2.23	krbPrincipalName.....	8-14
8.2.24	labeledURI .....	8-14
8.2.25	ldapSyntaxes.....	8-14
8.2.26	mail .....	8-15
8.2.27	matchingRules.....	8-15
8.2.28	middleName .....	8-15
8.2.29	modifiersName.....	8-16
8.2.30	modifyTimestamp .....	8-16
8.2.31	namingContexts .....	8-16
8.2.32	objectClass.....	8-17
8.2.33	objectClasses .....	8-17
8.2.34	objectClassMap .....	8-17
8.2.35	orclACI .....	8-18
8.2.36	orclACLResultsLatency .....	8-18
8.2.37	orclActivateReplication.....	8-19
8.2.38	orclActiveConn .....	8-19
8.2.39	orclActiveEndDate.....	8-19
8.2.40	orclActiveStartdate .....	8-20
8.2.41	orclActiveThreads.....	8-20
8.2.42	orclAgreementId .....	8-20
8.2.43	orclagreementtype .....	8-21
8.2.44	orclAnonymousBindsFlag.....	8-21
8.2.45	orclAppFullName .....	8-21
8.2.46	orclAppId .....	8-22
8.2.47	orclApplicationAddress.....	8-22
8.2.48	orclApplicationCommonName .....	8-22
8.2.49	orclApplicationType.....	8-23
8.2.50	orclAssocDB.....	8-23
8.2.51	orclAssocAsInstance .....	8-23
8.2.52	orclAttrACLEvalLatency .....	8-24
8.2.53	orclAudCustEvents .....	8-24
8.2.54	orclAudFilterPreset .....	8-24
8.2.55	orclAuditAttribute.....	8-25
8.2.56	orclAuditMessage.....	8-25
8.2.57	orclAudSplUsers .....	8-25
8.2.58	orclBERgenLatency.....	8-26
8.2.59	orclBlockDNIP.....	8-26
8.2.60	orlcachenotifyip.....	8-27
8.2.61	orclCatalogEntryDN.....	8-27
8.2.62	orclCategory .....	8-27
8.2.63	orclCertExtensionAttribute .....	8-28
8.2.64	orclCertExtensionOID .....	8-28
8.2.65	orclCertificateHash .....	8-28
8.2.66	orclCertificateMatch .....	8-29
8.2.67	orclCertMappingAttribute .....	8-29



8.2.68	orclChangeLogLife .....	8-30
8.2.69	orclChangeRetryCount .....	8-30
8.2.70	orclCommonAutoRegEnabled.....	8-30
8.2.71	orclCommonContextMap .....	8-31
8.2.72	orclCommonDefaultUserCreateBase.....	8-31
8.2.73	orclCommonGroupCreateBase.....	8-32
8.2.74	orclCommonNamingAttribute .....	8-32
8.2.75	orclCommonNicknameAttribute .....	8-32
8.2.76	orclCommonSASLRealm.....	8-33
8.2.77	orclCommonUserSearchBase.....	8-33
8.2.78	orclCommonVerifierEnable .....	8-33
8.2.79	orclCommonVerifierEnable .....	8-34
8.2.80	orclCompatibleVersion .....	8-34
8.2.81	orclComputedAttribute .....	8-34
8.2.82	orclconflresolution.....	8-35
8.2.83	orclConnectByAttribute .....	8-35
8.2.84	orclConnectBySearchBase.....	8-36
8.2.85	orclConnectByStartingValue.....	8-36
8.2.86	orclConnectionFormat .....	8-36
8.2.87	orclContact.....	8-37
8.2.88	orclCryptoScheme .....	8-37
8.2.89	orclDASAdminModifiable .....	8-37
8.2.90	orclDASAttrDispOrder .....	8-38
8.2.91	orclDASAttrName .....	8-38
8.2.92	orclDASEnableProductLogo .....	8-38
8.2.93	orclDASEnableSubscriberLogo.....	8-39
8.2.94	orclDASIsEnabled.....	8-39
8.2.95	orclDASIsMandatory .....	8-40
8.2.96	orclDASIsPersonal .....	8-40
8.2.97	orclDASLOV.....	8-40
8.2.98	orclDASPublicGroupDNs .....	8-41
8.2.99	orclDASSearchable .....	8-41
8.2.100	orclDASSearchColIndex .....	8-41
8.2.101	orclDASSearchFilter .....	8-42
8.2.102	orclDASSearchSizeLimit.....	8-42
8.2.103	orclDASSelfModifiable .....	8-42
8.2.104	orclDASUIType.....	8-43
8.2.105	orclDASURL .....	8-43
8.2.106	orclDASURLBase .....	8-44
8.2.107	orclDASValidatePwdReset.....	8-44
8.2.108	orclDASViewable.....	8-44
8.2.109	orcldataprivacymode .....	8-45
8.2.110	orclDateOfBirth.....	8-45
8.2.111	orclDBConnCreationFailed .....	8-45
8.2.112	orclDBLatency .....	8-46
8.2.113	orclDBSchemaIdentifier .....	8-46
8.2.114	orclDBType .....	8-46

8.2.115	orclDebugFlag .....	8-47
8.2.116	orclDebugForceFlush .....	8-47
8.2.117	orcldebuglevel .....	8-47
8.2.118	orclDebugOp .....	8-48
8.2.119	orclDefaultProfileGroup .....	8-48
8.2.120	orclDefaultSubscriber .....	8-49
8.2.121	orclDIMEonlyLatency .....	8-49
8.2.122	orclDIPRepository .....	8-49
8.2.123	orclDirectoryVersion .....	8-50
8.2.124	orclDirReplGroupAgreement .....	8-50
8.2.125	orclDirReplGroupDSAs .....	8-51
8.2.126	orclDisplayPersonalInfo .....	8-51
8.2.127	OrclDispThreads .....	8-51
8.2.128	orclDITRoot .....	8-52
8.2.129	orclDNSUnavailable .....	8-52
8.2.130	orclcachemaxsize .....	8-52
8.2.131	orclEcacheEnabled .....	8-53
8.2.132	orclEcacheHitRatio .....	8-53
8.2.133	orclEcacheMaxEntries .....	8-54
8.2.134	orclEcacheMaxSize .....	8-54
8.2.135	orclEcacheNumEntries .....	8-55
8.2.136	orclEcacheSize .....	8-55
8.2.137	orclEnabled .....	8-55
8.2.138	orclEnableGroupCache .....	8-56
8.2.139	orclencryptedattributes .....	8-56
8.2.140	orclEntryACLEvalLatency .....	8-56
8.2.141	orclEntryLevelACL .....	8-57
8.2.142	orclEventLevel .....	8-57
8.2.143	orclEventTime .....	8-58
8.2.144	orclEventType .....	8-58
8.2.145	orclExcludedAttributes .....	8-58
8.2.146	orclExcludedNamingContexts .....	8-59
8.2.147	orclFDIncreaseError .....	8-59
8.2.148	orclFilterACLEvalLatency .....	8-60
8.2.149	orclFlexAttribute1 .....	8-60
8.2.150	orclFlexAttribute2 .....	8-60
8.2.151	orclFlexAttribute3 .....	8-61
8.2.152	orclFrontLatency .....	8-61
8.2.153	orclGender .....	8-61
8.2.154	orclgeneratechangelog .....	8-62
8.2.155	orclGenObjLatency .....	8-62
8.2.156	orclGetNearACLLatency .....	8-62
8.2.157	orclGlobalID .....	8-63
8.2.158	orclGUID .....	8-63
8.2.159	orclGUPassword .....	8-63
8.2.160	orclHashedAttributes .....	8-64
8.2.161	orclHIQSchedule .....	8-64

8.2.162	orclHireDate .....	8-65
8.2.163	orclHostedCreditCardExpireDate.....	8-65
8.2.164	orclHostedCreditCardNumber.....	8-65
8.2.165	orclHostedCreditCardType.....	8-66
8.2.166	orclHostedDunsNumber .....	8-66
8.2.167	orclHostedPaymentTerm.....	8-66
8.2.168	orclHostname .....	8-67
8.2.169	orclIdleConn .....	8-67
8.2.170	orclIdleThreads .....	8-67
8.2.171	orclIncludedNamingContexts.....	8-68
8.2.172	orclIndexedAttribute.....	8-68
8.2.173	orclInitialServerMemSize .....	8-69
8.2.174	orclinmemfiltprocess.....	8-69
8.2.175	orclInterval.....	8-69
8.2.176	orclIpAddress.....	8-70
8.2.177	orclIsEnabled .....	8-70
8.2.178	orclIsVisible .....	8-70
8.2.179	orclLastAppliedChangeNumber.....	8-71
8.2.180	orclLastLoginTime.....	8-71
8.2.181	orclLDAPConnKeepALive.....	8-71
8.2.182	orclLDAPConnTimeout.....	8-72
8.2.183	orclLDAPInstanceID .....	8-72
8.2.184	orclLDAPProcessID.....	8-73
8.2.185	orclMaidenName .....	8-73
8.2.186	orclMappedDN .....	8-73
8.2.187	orclMaskFilter.....	8-74
8.2.188	orclMaskRealm.....	8-74
8.2.189	orclMasterNode .....	8-74
8.2.190	orclMatchDnEnabled .....	8-75
8.2.191	orclMaxCC .....	8-75
8.2.192	orclMaxConnInCache.....	8-76
8.2.193	orclmaxLatencyLog .....	8-76
8.2.194	orclMaxTcpIdleConnTime.....	8-76
8.2.195	orclMaxFDLimitReached.....	8-77
8.2.196	orclmaxfiltsize .....	8-77
8.2.197	OrclMaxLdapConns .....	8-77
8.2.198	orclmaxlogfiles .....	8-78
8.2.199	orclmaxlogfilesize .....	8-78
8.2.200	orclmaxpsearchconns .....	8-78
8.2.201	orclMaxProcessLimitReached.....	8-79
8.2.202	orclMaxServerRespTime.....	8-79
8.2.203	orclMemAllocError.....	8-79
8.2.204	orclMemberOf .....	8-80
8.2.205	orclNetDescName.....	8-80
8.2.206	orclNetDescString.....	8-81
8.2.207	orclNonSSLPort.....	8-81
8.2.208	orclNormDN.....	8-81

8.2.209	orclNWCongested .....	8-82
8.2.210	orclNwrwTimeout .....	8-82
8.2.211	orclNwUnavailable.....	8-83
8.2.212	orclObjectGUID.....	8-83
8.2.213	orclObjectSID .....	8-83
8.2.214	orclODIPAgent.....	8-84
8.2.215	orclODIPAgentConfigInfo .....	8-84
8.2.216	orclODIPAgentControl .....	8-85
8.2.217	orclODIPAgentExeCommand .....	8-85
8.2.218	orclODIPAgentHostName .....	8-86
8.2.219	orclODIPAgentName .....	8-86
8.2.220	orclODIPAgentPassword .....	8-86
8.2.221	orclODIPApplicationName.....	8-87
8.2.222	orclODIPApplicationsLocation.....	8-87
8.2.223	orclODIPAttributeMappingRules .....	8-87
8.2.224	orclODIPBootStrapStatus .....	8-88
8.2.225	orclODIPCommand.....	8-88
8.2.226	orclODIPConDirAccessAccount.....	8-88
8.2.227	orclODIPConDirAccessPassword .....	8-89
8.2.228	orclODIPConDirLastAppliedChgNum.....	8-89
8.2.229	orclODIPConDirMatchingFilter .....	8-90
8.2.230	orclODIPConDirURL .....	8-90
8.2.231	orclODIPConfigDNs .....	8-91
8.2.232	orclODIPConfigRefreshFlag .....	8-91
8.2.233	orclODIPDbConnectInfo .....	8-91
8.2.234	orclODIPEncryptedAttrKey.....	8-92
8.2.235	orclODIPEventFilter .....	8-92
8.2.236	orclODIPEventSubscriptions .....	8-92
8.2.237	orclODIPFilterAttrCriteria .....	8-93
8.2.238	orclODIPInstancesLocation.....	8-93
8.2.239	orclODIPInstanceStatus .....	8-93
8.2.240	orclODIPInterfaceType .....	8-94
8.2.241	orclODIPLastExecutionTime .....	8-94
8.2.242	orclODIPLastSuccessfulExecutionTime .....	8-95
8.2.243	orclODIPMustAttrCriteria.....	8-95
8.2.244	orclODIPObjectCriteria.....	8-95
8.2.245	orclODIPObjectDefnLocation .....	8-96
8.2.246	orclODIPObjectEvents .....	8-96
8.2.247	orclODIPObjectName.....	8-96
8.2.248	orclODIPObjectSyncBase.....	8-97
8.2.249	orclODIPOIDMatchingFilter.....	8-97
8.2.250	orclODIPOperationMode .....	8-97
8.2.251	orclODIPOptAttrCriteria.....	8-98
8.2.252	orclODIPPluginAddInfo.....	8-98
8.2.253	orclODIPPluginConfigInfo.....	8-98
8.2.254	orclODIPPluginEvents.....	8-99
8.2.255	orclODIPPluginExecData .....	8-99

8.2.256	orclODIPPluginExecName .....	8-99
8.2.257	orclODIPProfileDataLocation .....	8-100
8.2.258	orclODIPProfileDebugLevel .....	8-100
8.2.259	orclODIPProfileExecGroupID.....	8-101
8.2.260	orclODIPProfileInterfaceAdditionalInformation.....	8-101
8.2.261	orclODIPProfileInterfaceConnectInformation .....	8-102
8.2.262	orclODIPProfileInterfaceName.....	8-102
8.2.263	orclODIPProfileInterfaceType .....	8-102
8.2.264	orclODIPProfileInterfaceVersion.....	8-103
8.2.265	orclODIPProfileLastAppliedAppEventID .....	8-103
8.2.266	orclODIPProfileLastProcessingTime .....	8-103
8.2.267	orclODIPProfileLastSuccessfulProcessingTime .....	8-104
8.2.268	orclODIPProfileMaxErrors .....	8-104
8.2.269	orclODIPProfileMaxEventsPerInvocation .....	8-105
8.2.270	orclODIPProfileMaxEventsPerSchedule .....	8-105
8.2.271	orclODIPProfileMaxRetries.....	8-105
8.2.272	orclODIPProfileName .....	8-106
8.2.273	orclODIPProfileProcessingErrors.....	8-106
8.2.274	orclODIPProfileProcessingStatus .....	8-106
8.2.275	orclODIPProfileProvSubscriptionMode.....	8-107
8.2.276	orclODIPProfileSchedule.....	8-107
8.2.277	orclODIPProfileStatusUpdate.....	8-107
8.2.278	orclODIPProvEventCriteria .....	8-108
8.2.279	orclODIPProvEventLDAPChangeType .....	8-108
8.2.280	orclODIPProvEventObjectType.....	8-108
8.2.281	orclODIPProvEventRule .....	8-109
8.2.282	orclODIPProvEventRuleDTD .....	8-109
8.2.283	orclODIPProvInterfaceFilter .....	8-110
8.2.284	orclODIPProvInterfaceProcessor.....	8-110
8.2.285	orclODIPProvisioningAppGUID .....	8-110
8.2.286	orclODIPProvisioningAppName .....	8-111
8.2.287	orclODIPProvisioningEventMappingRules .....	8-111
8.2.288	orclODIPProvisioningEventPermittedOperations .....	8-112
8.2.289	orclODIPProvisioningEventSubscription .....	8-112
8.2.290	orclODIPProvisioningOrgGUID .....	8-113
8.2.291	orclODIPProvisioningOrgName .....	8-113
8.2.292	orclODIPProvProfileLocation .....	8-113
8.2.293	orclODIPRootLocation.....	8-114
8.2.294	orclODIPSchedulingInterval.....	8-114
8.2.295	orclODIPSchemaVersion .....	8-114
8.2.296	orclODIPSearchCountLimit .....	8-115
8.2.297	orclODIPSearchTimeLimit .....	8-115
8.2.298	orclODIPServerCommitSize.....	8-115
8.2.299	orclODIPServerConfigLocation.....	8-116
8.2.300	orclODIPServerDebugLevel.....	8-116
8.2.301	orclODIPServerRefreshIntvl .....	8-117
8.2.302	orclODIPServerSSLMode .....	8-117

8.2.303	orclODIPServerWalletLoc .....	8-117
8.2.304	orclODIPSynchronizationErrors.....	8-118
8.2.305	orclODIPSynchronizationMode .....	8-118
8.2.306	orclODIPSynchronizationStatus.....	8-118
8.2.307	orclODIPSyncProfileLocation .....	8-119
8.2.308	orclODIPSyncRetryCount .....	8-119
8.2.309	orclOidComponentName .....	8-120
8.2.310	orclOidInstanceName .....	8-120
8.2.311	orclOpAbandoned .....	8-120
8.2.312	orclOpCompleted .....	8-121
8.2.313	orclOpenConn .....	8-121
8.2.314	orclOpFailed .....	8-121
8.2.315	orclOpInitiated .....	8-122
8.2.316	orclOpLatency .....	8-122
8.2.317	orclOpPending .....	8-122
8.2.318	orclOpResult.....	8-123
8.2.319	orclOpSucceeded .....	8-123
8.2.320	orclOpTimedOut.....	8-123
8.2.321	orclOpTrackLevel.....	8-124
8.2.322	orclOpTrackMaxTotalSize.....	8-124
8.2.323	orclOpTrackNumElemContainers .....	8-124
8.2.324	orclORA28error .....	8-125
8.2.325	orclORA3113error .....	8-125
8.2.326	orclORA3114error .....	8-125
8.2.327	orclOracleHome .....	8-126
8.2.328	orclOwnerGUID.....	8-126
8.2.329	orclPassword .....	8-126
8.2.330	orclPasswordAttribute .....	8-127
8.2.331	orclPasswordHint .....	8-127
8.2.332	orclPasswordHintAnswer .....	8-127
8.2.333	orclPasswordVerifier.....	8-128
8.2.334	orclPilotMode .....	8-128
8.2.335	orclPKCS12Hint .....	8-129
8.2.336	orclPKIMatchingRule .....	8-129
8.2.337	orclPKINextUpdate .....	8-130
8.2.338	orclPKIValMecAttr .....	8-130
8.2.339	orclPluginAttributeList.....	8-130
8.2.340	orclPluginCheckEntryExist .....	8-131
8.2.341	orclPluginEnable.....	8-131
8.2.342	orclPluginEntryProperties.....	8-131
8.2.343	orclPluginIsReplace .....	8-132
8.2.344	orclPluginBinaryFlexfield.....	8-132
8.2.345	orclPluginFlexfield.....	8-132
8.2.346	orclPluginSecuredFlexfield .....	8-133
8.2.347	orclPluginKind .....	8-133
8.2.348	orclPluginLDAPOperation.....	8-134
8.2.349	orclPluginName .....	8-134

8.2.350	orclPluginPort .....	8-134
8.2.351	orclPluginRequestGroup .....	8-135
8.2.352	orclPluginRequestNegGroup .....	8-135
8.2.353	orclPluginResultCode .....	8-136
8.2.354	orclPluginSASLCallback .....	8-136
8.2.355	orclPluginSearchNotFound .....	8-137
8.2.356	orclPluginShareLibLocation .....	8-137
8.2.357	orclPluginSubscriberDNList .....	8-137
8.2.358	orclPluginTiming .....	8-138
8.2.359	orclPluginType .....	8-138
8.2.360	orclPluginVersion .....	8-139
8.2.361	OrclPluginWorkers .....	8-139
8.2.362	orclPrName .....	8-139
8.2.363	orclProductVersion .....	8-140
8.2.364	orclPrPassword .....	8-140
8.2.365	orclPurgeBase .....	8-140
8.2.366	orclPurgeDebug .....	8-141
8.2.367	orclPurgeEnable .....	8-141
8.2.368	orclPurgeFileLoc .....	8-141
8.2.369	orclPurgeFileName .....	8-142
8.2.370	orclPurgeFilter .....	8-142
8.2.371	orclPurgeInterval .....	8-142
8.2.372	orclPurgeNow .....	8-143
8.2.373	orclPurgePackage .....	8-143
8.2.374	orclPurgeSchedule .....	8-143
8.2.375	orclPurgeStart .....	8-144
8.2.376	orclPurgeTargetAge .....	8-144
8.2.377	orclPurgeTranSize .....	8-145
8.2.378	orclPwdAccountUnlock .....	8-145
8.2.379	orclPwdAllowHashCompare .....	8-145
8.2.380	orclPwdAlphaNumeric .....	8-146
8.2.381	orclPwdEncryptionEnable .....	8-146
8.2.382	orclPwdIllegalValues .....	8-147
8.2.383	orclPwdIPAccountLockedTime .....	8-147
8.2.384	orclPwdIPFailureTime .....	8-147
8.2.385	orclPwdIPLockout .....	8-148
8.2.386	orclPwdIPLockoutDuration .....	8-148
8.2.387	orclPwdIPMaxFailure .....	8-148
8.2.388	orclpwdmaxinactivitytime .....	8-149
8.2.389	orclPwdMaxRptchars .....	8-149
8.2.390	orclPwdMinAlphachars .....	8-150
8.2.391	orclPwdMinSpecialchars .....	8-150
8.2.392	orclPwdMinUppercase .....	8-150
8.2.393	orclpwdminlowercase .....	8-151
8.2.394	orclPwdPolicyEnable .....	8-151
8.2.395	orclPwdTrackLogin .....	8-151
8.2.396	orclPwdVerifierParams .....	8-152

8.2.397	orclQueueDepth.....	8-152
8.2.398	orclQueueLatency.....	8-152
8.2.399	orclReadWaitThreads.....	8-153
8.2.400	orclReqAttrCase.....	8-153
8.2.401	orclrefreshdgrmems.....	8-154
8.2.402	orclReplAgreements.....	8-154
8.2.403	orclReplAttrConfl.....	8-154
8.2.404	orclreplautotune.....	8-155
8.2.405	orclReplicaDN.....	8-155
8.2.406	orclReplicaID.....	8-155
8.2.407	orclReplicaSecondaryURI.....	8-156
8.2.408	orclReplicaState.....	8-156
8.2.409	orclreplicationid.....	8-157
8.2.410	orclReplicationProtocol.....	8-157
8.2.411	orclReplicationState.....	8-157
8.2.412	orclReplicaType.....	8-158
8.2.413	orclReplicaURI.....	8-158
8.2.414	orclReplicaVersion.....	8-158
8.2.415	orclreplmaxworkers.....	8-159
8.2.416	orclreplusesasl;digest-md5.....	8-159
8.2.417	orclResourceIdentifier.....	8-159
8.2.418	orclResourceName.....	8-160
8.2.419	orclResourceTypeName.....	8-160
8.2.420	orclResourceViewers.....	8-160
8.2.421	orclRevPwd.....	8-161
8.2.422	orclrienabled.....	8-161
8.2.423	orclrscacheattr.....	8-161
8.2.424	orclTraceConnDN.....	8-162
8.2.425	orclTraceConnIP.....	8-162
8.2.426	orclSAMAccountName.....	8-163
8.2.427	orclSASLAAuthenticationMode.....	8-163
8.2.428	orclSASLCipherChoice.....	8-164
8.2.429	orclSASLMechanism.....	8-164
8.2.430	orclsDumpFlag.....	8-164
8.2.431	orclSearchBaseDN.....	8-165
8.2.432	orclSearchFilter.....	8-165
8.2.433	orclSearchScope.....	8-165
8.2.434	orclSecondaryUID.....	8-166
8.2.435	orclSequence.....	8-166
8.2.436	orclServerAvgMemGrowth.....	8-166
8.2.437	orclServerMode.....	8-167
8.2.438	orclServerProcs.....	8-167
8.2.439	orclServiceInstanceLocation.....	8-167
8.2.440	orclServiceMember.....	8-168
8.2.441	orclServiceSubscriptionLocation.....	8-168
8.2.442	orclServiceSubType.....	8-168
8.2.443	orclServiceType.....	8-169



8.2.444	orclSID .....	8-169
8.2.445	orclsimplemodchglogattributes .....	8-170
8.2.446	orclSizeLimit .....	8-170
8.2.447	orclSkewedAttribute .....	8-170
8.2.448	orclSkipRefInSQL .....	8-171
8.2.449	orclSMSpec.....	8-171
8.2.450	orclSQLexeFetchLatency .....	8-171
8.2.451	orclSQLGenReusedParsed.....	8-172
8.2.452	orclSSLAuthentication .....	8-172
8.2.453	orclSSLCipherSuite.....	8-173
8.2.454	orclSSLEnable .....	8-173
8.2.455	orclsslinteropmode .....	8-174
8.2.456	orclSSLPort .....	8-174
8.2.457	orclSSLVersion .....	8-175
8.2.458	orclSSLWalletURL .....	8-175
8.2.459	orclStatsDN.....	8-175
8.2.460	orclStatsFlag.....	8-176
8.2.461	orclStatsLevel .....	8-176
8.2.462	orclStatsOp.....	8-177
8.2.463	orclStatsPeriodicity .....	8-177
8.2.464	orclStatus.....	8-177
8.2.465	orclSUAccountLocked.....	8-178
8.2.466	orclSubscriberDisable.....	8-178
8.2.467	orclSubscriberFullName .....	8-178
8.2.468	orclSubscriberNickNameAttribute .....	8-179
8.2.469	orclSubscriberSearchBase .....	8-179
8.2.470	orclSubscriberType .....	8-179
8.2.471	orclSuffix .....	8-180
8.2.472	orclSuiteType.....	8-180
8.2.473	orclSULoginFailureCount.....	8-180
8.2.474	orclSUName.....	8-181
8.2.475	orclSUPassword .....	8-181
8.2.476	orclSystemName .....	8-182
8.2.477	orclTcpConnToClose.....	8-182
8.2.478	orclTcpConnToShutDown.....	8-182
8.2.479	orclThreadSpawnFailed.....	8-183
8.2.480	orclThreadsPerSupplier .....	8-183
8.2.481	orclTimeLimit.....	8-183
8.2.482	orclTimeZone .....	8-184
8.2.483	orclTLimitMode .....	8-184
8.2.484	orclTotFreePhyMem.....	8-184
8.2.485	orclTraceDimesionLevel .....	8-185
8.2.486	orclTraceFileLocation .....	8-185
8.2.487	orclTraceFileSize .....	8-185
8.2.488	orclTraceLevel .....	8-186
8.2.489	orclTraceMode.....	8-186
8.2.490	orclTrustedApplicationGroup .....	8-186

8.2.491	orclTraceMode.....	8-187
8.2.492	orclTxnMaxOperations .....	8-187
8.2.493	orclTxnTimeLimit .....	8-187
8.2.494	orclUIAccessibilityMode .....	8-188
8.2.495	orclUniqueAttrName .....	8-188
8.2.496	orclUniqueEnable .....	8-189
8.2.497	orclUniqueObjectClass.....	8-189
8.2.498	orclUniqueScope .....	8-189
8.2.499	orclUniqueSubtree.....	8-190
8.2.500	orclUnsyncRevPwd .....	8-190
8.2.501	orclUpdateSchedule .....	8-191
8.2.502	orclUpgradeInProgress.....	8-191
8.2.503	orclUserDN.....	8-191
8.2.504	orclUserIDAttribute.....	8-192
8.2.505	orclUserModifiable.....	8-192
8.2.506	orclUserObjectClasses .....	8-192
8.2.507	orclUserPrincipalName .....	8-193
8.2.508	orclVersion.....	8-193
8.2.509	orclWirelessAccountNumber.....	8-193
8.2.510	orclWorkflowNotificationPref .....	8-194
8.2.511	orclWriteWaitThreads.....	8-194
8.2.512	owner .....	8-194
8.2.513	pilotStartTime.....	8-195
8.2.514	preferredServerList.....	8-195
8.2.515	profileTTL .....	8-195
8.2.516	protocolInformation .....	8-196
8.2.517	pwdAccountLockedTime .....	8-196
8.2.518	pwdAllowUserChange .....	8-197
8.2.519	pwdChangedTime .....	8-197
8.2.520	pwdCheckSyntax .....	8-197
8.2.521	pwdExpirationWarned .....	8-198
8.2.522	pwdExpireWarning.....	8-198
8.2.523	pwdFailureCountInterval.....	8-199
8.2.524	pwdFailureTime .....	8-199
8.2.525	pwdGraceLoginLimit.....	8-199
8.2.526	pwdGraceLoginTimeLimit.....	8-200
8.2.527	pwdGraceUseTime .....	8-200
8.2.528	pwdHistory.....	8-201
8.2.529	pwdInHistory.....	8-201
8.2.530	pwdLockout.....	8-201
8.2.531	pwdLockoutDuration.....	8-202
8.2.532	pwdMaxAge.....	8-202
8.2.533	pwdMaxFailure.....	8-203
8.2.534	pwdMinAge.....	8-203
8.2.535	pwdMinLength .....	8-204
8.2.536	pwdMustChange .....	8-204
8.2.537	pwdpolicysubentry.....	8-204

8.2.538	pwdReset.....	8-205
8.2.539	pwdSafeModify.....	8-205
8.2.540	ref .....	8-205
8.2.541	seeAlso.....	8-206
8.2.542	serverName.....	8-206
8.2.543	serviceAuthenticationMethod .....	8-206
8.2.544	serviceCredentialLevel.....	8-207
8.2.545	serviceSearchDescriptor.....	8-207
8.2.546	sn .....	8-207
8.2.547	supportedcontrol .....	8-208
8.2.548	supportedextension .....	8-208
8.2.549	supportedldapversion.....	8-208
8.2.550	uniqueMember.....	8-208
8.2.551	supportedsaslmmechanisms .....	8-209
8.2.552	userCertificate;binary .....	8-209
8.2.553	userPassword .....	8-209
8.2.554	userPKCS12 .....	8-210
8.2.555	x509issuer.....	8-210

## Part III   Appendixes

### A   LDIF File Format

A.1	General LDIF Formatting Rules.....	A-1
A.1.1	Line Types and White Space .....	A-1
A.1.2	Sequencing of Entries.....	A-2
A.1.3	Binary Files .....	A-2
A.1.4	Non-Printing Characters in Attribute Values.....	A-2
A.2	LDIF Format for Entries .....	A-2
A.2.1	LDIF Format for Adding Entries .....	A-3
A.2.2	LDIF Format for Deleting Entries.....	A-3
A.2.3	LDIF Format for Modifying Entries .....	A-4
A.2.4	LDIF Format for Modifying the RDN of an Entry .....	A-4
A.2.5	LDIF Format for Modifying the DN of an Entry.....	A-5
A.3	LDIF Format for Adding Schema Elements.....	A-5
A.4	LDIF Format for Migrating Entries .....	A-6
A.4.1	Substitution Variables for Migration Input Files .....	A-6
A.4.1.1	Predefined Substitution Variables .....	A-7
A.4.2	Reconcile Options for Migrated Entries .....	A-8

## List of Tables

3-1	Error Messages of the Data Migration Tool .....	3-50
4-1	Default Values for the entos Argument.....	4-10
4-2	Default Values for the entod Argument.....	4-10
4-3	Default Values for the atos Argument .....	4-11
4-4	Default Values for the atrod Argument.....	4-12
4-5	Default Values for the svatrdif Argument .....	4-13
4-6	Default Values for the mvatrdif Argument.....	4-13
4-7	Default Values for the mvatrdif Argument.....	4-14
4-8	Default Values for the odefos Argument .....	4-15
4-9	Default Values for the odefod Argument.....	4-15
4-10	Default Values for the odefdif Argument .....	4-16
4-11	Default Values for the adefos Argument.....	4-16
4-12	Default Values for the adefod Argument.....	4-16
4-13	Default Values for the adefdif Argument.....	4-17
6-1	Attribute Syntax Commonly Used in Oracle Internet Directory .....	6-3
6-2	Request Controls Supported by Oracle Internet Directory .....	6-8
6-3	Response Controls Supported by Oracle Internet Directory.....	6-13
7-1	Standard LDAP Object Classes Used By Oracle Internet Directory.....	7-1
8-1	Standard LDAP Attributes Used By Oracle Internet Directory .....	8-1
8-2	Event Levels.....	8-57
8-3	SSL Cipher Suites Supported in Oracle Internet Directory .....	8-173
A-1	Predefined Substitution Variables.....	A-7

---

---

# Preface

The *Oracle Fusion Middleware Reference for Oracle Identity Management* provides reference information about the command-line tools and LDAP directory schema elements for Oracle Identity Management components.

## Audience

The *Oracle Fusion Middleware Reference for Oracle Identity Management* is intended for administrators, developers, and others who perform administration tasks for Oracle Identity Management components. You should be familiar with either the UNIX operating system or the Microsoft Windows operating system in order to understand the command-line syntax and examples. You also must be familiar with the Lightweight Directory Access Protocol (LDAP).

## Documentation Accessibility

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

### Access to Oracle Support

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

## Related Documents

For more information, see the following manuals in the Oracle Identity Management 11g Release 1 (11.1.1) documentation set:

- *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Directory Integration Platform*
- *Oracle Fusion Middleware Application Developer's Guide for Oracle Identity Management*

## Conventions

The following text conventions are used in this document:

<b>Convention</b>	<b>Meaning</b>
<b>boldface</b>	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
<i>italic</i>	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

---

## Command-Line Tool Reference

Part 1 of the *Oracle Fusion Middleware Reference for Oracle Identity Management* contains information about the command-line tools for Oracle Identity Management.

Part I contains the following chapters:

- Chapter 1, "Command-Line Tools Overview"
- Chapter 2, "Oracle Internet Directory Administration Tools"
- Chapter 3, "Oracle Internet Directory Data Management Tools"
- Chapter 4, "Oracle Internet Directory Replication Management Tools"
- Chapter 5, "Oracle Directory Integration Platform Tools"





---

---

# Command-Line Tools Overview

This chapter provides an overview of the command-line tools available for Oracle Identity Management.

This chapter includes the following sections:

- Section 1.1, "Using Passwords with Command-Line Tools"
- Section 1.2, "Configuring Your Environment"
- Section 1.3, "Oracle Identity Management Command-Line Tool Categories"

## 1.1 Using Passwords with Command-Line Tools

Many command-line tools require you to authenticate by providing a password. In some cases, you can provide the password in either of two ways:

- In response to a prompt from the command.
- Following an option on the command line

For security reasons, avoid supplying a password on the command line whenever possible. A password typed on the command line is visible on your screen and might appear in output from the `ps` command or in log files. When you supply a password at a prompt, it is not visible on the screen, in output from the `ps` command, or in log files.

The LDAP tools have been modified to disable the options `-w password` and `-P password` when the environment variable `LDAP_PASSWORD_PROMPTONLY` is set to `TRUE` or `1`. If you use `-q` or `-Q`, respectively, the command prompts you for the user password or wallet password. Set this environment variable whenever possible. This feature affects the behavior of the following tools:

- Section 3.5, "ldapadd" (LDAP Data Add Tool)
- Section 3.6, "ldapaddmt" (Multi-Threaded LDAP Data Add Tool)
- Section 3.7, "ldapbind" (Authentication Validation Tool)
- Section 3.8, "ldapcompare" (Attribute Comparison Tool)
- Section 3.9, "ldapdelete" (LDAP Data Deletion Tool)
- Section 3.10, "ldapmoddn" (LDAP DN/RDN Modification Tool)
- Section 3.11, "ldapmodify" (LDAP Data Modification Tool)
- Section 3.12, "ldapmodifymt" (Multi-Threaded LDAP Data Modification Tool)
- Section 3.13, "ldapsearch" (LDAP Search Tool)

---

---

**Note:** When you use the `-q` or `-Q` option and redirect or pipe the output of an LDAP command, you do not see the prompt on the command line. The command still accepts the password you provide. If there is no wallet password and you are using the `-Q` option, when prompted for the password, hit Enter.

---

---

If you use the `-w password` option with an LDAP tool when the environment variable `LDAP_PASSWORD_PROMPTONLY` is set to true, you see the following error message, followed by command usage help.

Command-line passwords are disabled for LDAP commands.  
Use `-q` option instead of `-w <password>`. You are prompted for the password.\*

Similarly, If you use the `-P password` option with an LDAP tool when the environment variable `LDAP_PASSWORD_PROMPTONLY` is set to true, you see the following error message, followed by command usage help.

Command-line passwords are disabled for LDAP commands.  
Use `-Q` option instead of `-P <password>`. You are prompted for the password.

## 1.2 Configuring Your Environment

Before you begin using the Oracle Identity Management command-line tools, you must configure your environment. This involves setting the appropriate environment variables.

The syntax and examples provided in this guide require that you have the following environment variables set:

- `ORACLE_HOME` - The location of non-writable files in your Oracle Identity Management installation.
- `ORACLE_INSTANCE` - The location of writable files in your Oracle Identity Management installation.
- `NLS_LANG` (`APPROPRIATE_LANGUAGE.AL32UTF8`) - The default language set at installation is `AMERICAN_AMERICA`.
- `WLS_HOME` - The location where the WebLogic Server is installed. This environment variable is required for Oracle Directory Integration Platform commands but not Oracle Internet Directory commands.
- `PATH` - The following directory locations should be added to your `PATH`:

`ORACLE_HOME/bin`

`ORACLE_HOME/ldap/bin`

`ORACLE_HOME/ldap/admin`

## 1.3 Oracle Identity Management Command-Line Tool Categories

The Oracle Identity Management command-line tools are organized into the following categories:

- [Chapter 2, "Oracle Internet Directory Administration Tools"](#)
- [Chapter 3, "Oracle Internet Directory Data Management Tools"](#)
- [Chapter 4, "Oracle Internet Directory Replication Management Tools"](#)

- Chapter 5, "Oracle Directory Integration Platform Tools"



---

---

# Oracle Internet Directory Administration Tools

This chapter describes the command-line tools used to administer Oracle Internet Directory.

This chapter includes the following sections:

- Section 2.1, "oidpasswd" (Database Password Utility)
- Section 2.2, "oidctl" (Oracle Internet Directory Control)
- Section 2.3, "oiddiag" (Oracle Internet Directory Server Diagnostic Tool)
- Section 2.4, "oidmon" (Oracle Internet Directory Monitor)
- Section 2.5, "opmnctl" (Oracle Process Manager and Notification Server Control)
- Section 2.6, "oidstats.sql" (Oracle Internet Directory Database Statistics Collection Tool)
- Section 2.7, "oidcred" (Oracle Internet Directory Credential Management Tool)
- Section 2.8, "oidrealm" (Oracle Internet Directory Realm Creation Tool)

---

---

**Note:** The term "instance" refers to an Oracle instance in `opmnctl` documentation. The term "instance" refers to an Oracle Internet Directory instance in `oidctl` documentation.

---

---

## 2.1 oidpasswd

The Oracle Internet Directory Database Password Utility (`oidpasswd`) is used to:

- Change the password to the Oracle Internet Directory database.  
Oracle Internet Directory uses a password when connecting to an Oracle database. The default for this password matches the value you specified during installation for the Oracle Fusion Middleware administrator's password. You can change this password by using the OID Database Password Utility.
- Create wallets for the Oracle Internet Directory database password and the Oracle directory replication server password.
- Unlock or reset the directory superuser account, namely, `cn=orcladmin`.
- Reset an access control point (ACP) so that the subtree is accessible by the Oracle Internet Directory superuser.
- Manage the restricted superuser ACL.

## 2.1.1 Syntax for oidpasswd

```
oidpasswd [connect=connect_string] [change_oiddb_pwd=true | create_wallet=true |  
unlock_su_acct=true | reset_su_password=true | manage_su_acl=true]
```

## 2.1.2 Arguments for oidpasswd

### **connect=connect\_string**

Required. The directory database connect string. If you already have a `tnsnames.ora` file configured, then this is the net service name specified in that file, which is located by default in `ORACLE_HOME/config`. (You can set the `TNS_ADMIN` environment variable if you want to use a different location.)

### **change\_oiddb\_pwd=true | unlock\_su\_acct=true | reset\_su\_password=true | manage\_su\_password=true**

Required. The operation you want to perform. Depending on the operation you choose, the Oracle Internet Directory Database Password Utility prompts you for additional information. The following choices are available:

- `change_oiddb_pwd=true` - Changes the password to the Oracle Internet Directory database. You are prompted to provide the current database password, enter a new database password, and confirm the new password.

---

---

**Note:** In an Oracle Real Application Clusters (Oracle RAC) environment, if you update the password on one Oracle RAC node, then you must update the wallet on the other Oracle RAC nodes. Refer to "About Changing the ODS Password on an Oracle RAC System" in the *Oracle Application Server High Availability Guide* for more information.

---

---

- `create_wallet=true` - Create a wallet named `oidpwdlldap1` for the Oracle Internet Directory database password, and a wallet, named `oidpwdrsid`, for the Oracle directory replication server password.

The `sid` is obtained from the connected database.

You must provide the ODS password to authenticate yourself to the ODS database before the ODS wallet can be generated. Note that the default ODS password is the same as that for the Oracle Fusion Middleware administrator.

- `unlock_su_acct=true` - Unlocks a superuser account that has been locked.
- `reset_su_password=true` - Resets the password for the Oracle Internet Directory superuser account. You are prompted to provide the Oracle Internet Directory database password, enter a new superuser password, and confirm the new superuser password.
- `manage_su_acl=true` - Manages the restricted superuser ACL.

## 2.1.3 Tasks and Examples for oidpasswd

Using Oracle Internet Directory Database Password Utility, you can perform the following tasks:

- [Changing the Password to the Oracle Internet Directory Database](#)
- [Creating Wallets for Directory Database and Replication Server Passwords](#)

- Section 2.1.3.3, "Unlocking the Superuser Account"
- Section 2.1.3.4, "Resetting the Superuser Password"
- Section 2.1.3.5, "Managing Superuser Access Control Points"

### 2.1.3.1 Changing the Password to the Oracle Internet Directory Database

The following example shows how to change the Oracle Internet Directory database password, assuming the database is on the same machine.

#### Example:

```
oidpasswd
current password: oldpassword
new password: newpassword
confirm password: newpassword
password set.
```

The Oracle Internet Directory Database Password Utility prompts you for the current password. Type the current password, then the new password, then a confirmation of the new password.

---



---

#### Notes:

- User responses are not echoed to the screen when you enter a password.
  - Whenever you change the password to the Oracle Internet Directory database by using the OID Database Password Utility, you should also run the `oidempasswd` utility. This enables the Oracle Enterprise Manager Daemon (a component of Oracle Enterprise Manager) to properly cache that password and contact the ODS schema upon starting up. Once you have run the `oidempasswd` utility, you can monitor Oracle Internet Directory processes from the Oracle Enterprise Manager.
- 
- 

### 2.1.3.2 Creating Wallets for Directory Database and Replication Server Passwords

The following example shows how to create wallets for the Oracle Internet Directory database password and the Directory Replication server password.

#### Example:

```
oidpasswd connect=dbs1 create_wallet=true
```

The argument `create_wallet=true` is mandatory in this case. Except for the connect string, no other option can be specified.

### 2.1.3.3 Unlocking the Superuser Account

The following example shows how to unlock the Oracle Internet Directory superuser account, `cn=orcladmin`.

#### Example:

```
oidpasswd connect=dbs1 unlock_su_acct=true
```

The argument `unlock_su_acct` is mandatory. Except for connect string, no other option can be specified.

### 2.1.3.4 Resetting the Superuser Password

If you forget the Oracle Internet Directory superuser password, you can use the `oidpasswd` tool to reset it. You must provide the Oracle Internet Directory database password. When you first install Oracle Internet Directory, the superuser password and Oracle Internet Directory database password are the same. After installation, however, you can change the Oracle Internet Directory superuser password using `ldapmodify`. You can change the Oracle Internet Directory superuser password using the `oidpasswd` tool separately.

The following example shows how to reset the Oracle Internet Directory superuser password. The `oidpasswd` tool prompts you for the Oracle Internet Directory database password.

#### Example:

```
oidpasswd connect=dbs1 reset_su_password=true
OID DB user password: oid_db_password
      password: new_su_password
confirm password: new_su_password
OID super user password reset successfully
```

### 2.1.3.5 Managing Superuser Access Control Points

When an access control point (ACP) is set with an access control item (ACI) that has the keyword `DenyGroupOverride`, neither the Oracle Internet Directory superuser nor members of `DirectoryAdminGroup` can access the subtree under that ACP. If necessary, you can use the `oidpasswd` tool to reset that ACP so that the subtree is accessible by the Oracle Internet Directory superuser.

The following example shows how to reset a restricted ACP. The `oidpasswd` utility prompts you to enter the Oracle Internet Directory database password and to choose which superuser restricted ACPs to reset.

#### Example:

```
oidpasswd conn=dbs1 manage_su_acl=true
OID DB user password: oid_db_password
```

```
The super user restricted ACP list
[1] o=oracle,c=us
[2] ou=personnel,o=oracle,c=us
```

```
Enter 'resetall' or the number(s) of the ACP to be reset separated by [,]
resetall
```

Once you have reset some ACPs so that the superuser can access them, you can use `ldapmodify` to make the subtrees inaccessible to the superuser again.

## 2.1.4 Related Command-Line Tools for `oidpasswd`

- See [Section 3.11, "ldapmodify."](#)
- See [Section 2.4, "oidmon."](#)

## 2.2 oidctl

Oracle Internet Directory Control Utility (`oidctl`) is a command-line tool for starting and stopping Oracle Identity Management server instances. In 11g Release 1 (11.1.1), it



is typically used only to configure, start, and stop the Oracle Directory Replication Server.

---



---

#### Notes:

- You must set the environment variables `ORACLE_INSTANCE`, `ORACLE_HOME`, `INSTANCE_NAME` and `COMPONENT_NAME` before you run the `oidctl` command. Alternatively, you can pass the instance name and component name in the command line as `name=instanceName, componentname=componentName`.
  - Best practice is to create new Oracle Internet Directory instances by creating new Oracle Internet Directory components with `opmnctl createcomponent`. See [Section 2.5, "opmnctl"](#). You should use `oidctl` to create an instance *only if* you plan to run Oracle Internet Directory in standalone mode and not use Oracle Enterprise Manager Fusion Middleware Control.
  - The term "instance" refers to an Oracle Internet Directory instance in `oidctl` command documentation.
- 
- 

The commands issued by Oracle Internet Directory Control Utility are interpreted and executed by the Oracle Internet Directory Monitor process. Before starting a server instance with this utility, make sure that the Monitor process is running. See [Section 2.4, "oidmon"](#).

## 2.2.1 Syntax for oidctl

```
oidctl [connect=connect_string] { server=OIDLDAPD | OIDREPLD }
instance=instance_number [name=instance_name] [componentname=component_name]
[host=host_name] [flags="flagname=value ..." ] [
{start | stop | add | delete | status [-diag | -odiag interval]}
```

## 2.2.2 Arguments for oidctl

### **connect=connect\_string**

Required. The directory database connect string. If you already have a `tnsnames.ora` file configured, then this is the net service name specified in that file, which is located by default in `ORACLE_INSTANCE/config`. (You can set the `TNS_ADMIN` environment variable if you want to use a different location.)

### **server=server**

Required. The options are:

- `OIDLDAPD` — Oracle Internet Directory server
- `OIDREPLD` — Directory Replication server

### **instance=instance\_number**

Required. The numerical value of the instance. The value must be greater than 0 but less than 100.

### **host=host\_name**

Optional. Name of the logical host where the server is located or will be added. If you are using this argument, make sure `oidmon` is also started with the `host=host_name`

parameter. If `oidmon` is started by `opmn`, then make sure the `hostname` parameter exists in the file `ORACLE_INSTANCE/config/OPMN/opmn/opmn.xml`.

**name=instance\_name**

Optional. Name of the instance to be used. The default is `inst1`.

**componentname=component\_name**

Optional. Name of the component to be used. The default is `oid1`.

**flags="flagname=value | -flag value..."**

The flags argument is needed only while starting the server. If the flags consist of UNIX-style keywords, then the keyword-value pairs must be separated by spaces.

- [Section 2.2.2.1, "OIDLDAPD Flags"](#)
- [Section 2.2.2.2, "OIDREPLD Flags"](#)

**start | stop | restart | add | delete | status**

Required. The operation to perform on the given server process.

- `start` — Start the server=*server* instance=*instance\_number* [*name=instance\_name* *componentName=component\_name*]
- `stop` — Stop the server=*server* instance=*instance\_number* [*name=instance\_name* *componentName=component\_name*]
- `add` — Add the instance-specific configuration entry and start the server instance.
- `delete` — Stop the server instance and delete the instance-specific configuration entry
- `status [-diag | -opdiag]` — Report the status of running server instances. Use `-diag` with `status` to get diagnostic information. Use `-opdiag`, followed by *interval*, an integer value, with `status` to get the operation count for each operation for each Oracle Internet Directory component.

### 2.2.2.1 OIDLDAPD Flags

In 11g Release 1 (11.1.1), the recommended tool for creating instances and managing the LDAP server is `opmnctl`, not `oidctl`. See [Section 2.5, "opmnctl"](#). You should only use `oidctl` for these purposes if you plan to run Oracle Internet Directory in standalone mode and never use Oracle Enterprise Manager Fusion Middleware Control.

**-l true | false**

Optional. Turns replication change logging on or off. Use `true` to enable change logging. Use `false` to disable change logging. The default is `true`. This option has effect only when creating an Oracle Internet Directory instance.

**-p ldap\_port**

Optional. Specifies the LDAP port that this Oracle Internet Directory server instance will use. If not specified the default 3060 is used.

**-server number\_of\_processes**

The number of server processes to start on this port.

**-sport ssl\_port**

Optional. Specifies the LDAPS port that this Oracle Internet Directory server instance will use. If not specified the default 3133 is used.

**-work maximum\_threads**

The maximum number of worker threads for this server.

**2.2.2.2 OIDREPLD Flags****-p directory\_port\_number**

Required for a start operation. Port number used to connect to Oracle Internet Directory server. The default is 3060.

**-h directory\_hostname**

Required for a start operation. The host name of the Oracle Internet Directory server to which the replication server connects. If not specified, localhost is used.

**-m true | false**

Optional. Use `true` to enable conflict resolution. Use `false` to disable conflict resolution. The default value is `true`.

**-sizelimit transaction\_size**

Optional. The number of changes applied in each replication update cycle. If not specified the value from the Oracle Internet Directory server size limit configuration parameter, which has a default of 1024.

**2.2.3 Tasks and Examples for oidctl**

In 11g Release 1 (11.1.1), `oidctl` is used primarily to manage the replication server. The recommended tool for creating instances and managing the LDAP server is `opmnctl`, not `oidctl`. See [Section 2.5, "opmnctl"](#). You should only use `oidctl` for these purposes if you plan to run Oracle Internet Directory in standalone mode and never use Oracle Enterprise Manager Fusion Middleware Control.

Before using Oracle Internet Directory Control, make sure that Oracle Internet Directory Monitor is running. To verify this on UNIX, enter the following at the command-line:

```
ps -ef | grep oidmon
```

See [Section 2.4, "oidmon"](#) for more information about Oracle Internet Directory Monitor.

Using Oracle Internet Directory Control, you can perform the following tasks:

- [Section 2.2.3.1, "Creating an Oracle Internet Directory Instance in an Existing Component"](#)
- [Section 2.2.3.2, "Deleting an Oracle Internet Directory Instance in a Component"](#)
- [Section 2.2.3.3, "Starting an Oracle Internet Directory Server Instance"](#)
- [Section 2.2.3.4, "Stopping an Oracle Internet Directory Server Instance"](#)
- [Section 2.2.3.5, "Restarting an Oracle Internet Directory Server Instance"](#)
- [Section 2.2.3.6, "Starting a Directory Replication Server Instance"](#)

- Section 2.2.3.7, "Stopping a Directory Replication Server Instance"
- Section 2.2.3.8, "Starting and Stopping a Server Instance on a Virtual Host or Cluster Node"
- Section 2.2.3.9, "Reporting the Status of Each Server"
- Section 2.2.3.10, "Reporting Diagnostics"
- Section 2.2.3.11, "Reporting Server Manageability Information"

### 2.2.3.1 Creating an Oracle Internet Directory Instance in an Existing Component

To create another Oracle Internet Directory instance within an existing component, type

```
oidctl connect=connect_string server=oidldapd inst=new_instance_number \
  name=instanceName componentname=componentName \
  flags=port=non_ssl_port sport=ssl_port add
```

The name and component name arguments are required unless the environment variables `INSTANCE_NAME` and `COMPONENT_NAME` have been set. Typically, the `inst` value of the original instance is 1, the second instance you create is 2, and so forth.

As an example:

```
oidctl connect=oiddb server=oidldapd inst=2 "flags=port=5678 sport=5679" add
```

### 2.2.3.2 Deleting an Oracle Internet Directory Instance in a Component

To delete one Oracle Internet Directory instance within a component, type

```
oidctl connect=connect_string server=oidldapd inst=new_instance_number \
  name=instanceName componentname=componentName \
  flags=port=non_ssl_port sport=ssl_port delete
```

Typically, the `inst` value of the original instance is 1, the second instance you create is 2, and so forth.

### 2.2.3.3 Starting an Oracle Internet Directory Server Instance

When starting an Oracle Internet Directory server, you must supply the instance, `server=OIDLDAPD`, and `start` arguments. All other arguments are optional.

Before starting a new instance of `OIDLDAPD`, run the command:

```
oidctl connect=connstr status
```

to make sure `oidmon` is running and that the instance number and ports that you intend to use are not already in use.

#### Example:

```
oidctl connect=dbs1 server=OIDLDAPD instance=2 flags="-p 3133 \
  -debug 1024 -l false" start
```

### 2.2.3.4 Stopping an Oracle Internet Directory Server Instance

#### Example:

```
oidctl connect=dbs1 server=OIDLDAPD instance=2 stop
```

### 2.2.3.5 Restarting an Oracle Internet Directory Server Instance

A restart operation is useful when you want to refresh the server cache immediately, or when you have changed a configuration set entry and want your changes to take effect on an active server instance. When the Oracle Internet Directory server restarts, it maintains the same arguments it had before it stopped.

For example, if you changed a configuration set that was being referenced by an active instance of Oracle Internet Directory server, you could update it by restarting that server instance. You do not need to supply the `configset` argument again, as it is maintained from the prior start operation.

#### Example:

```
oidctl connect=dbs1 server=OIDLDAPD instance=1 restart
```

To restart all active instances on a node, do not specify the `instance` argument. Note that a server is momentarily unavailable to client requests during a restart.

### 2.2.3.6 Starting a Directory Replication Server Instance

When starting an Oracle Directory Replication server, you must supply the information it needs to connect to the Oracle Internet Directory server. You cannot use the `add` option when starting a replication server.

#### Example:

```
oidctl connect=dbs1 server=OIDREPL instance=1 flags="-p 3060 \  
-h ldaphost.example.com -d 1024" start
```

This command uses the same instance-specific configuration entry as `instance=1`.

### 2.2.3.7 Stopping a Directory Replication Server Instance

#### Example:

```
oidctl connect=dbs1 server=OIDREPLD instance=1 stop
```

### 2.2.3.8 Starting and Stopping a Server Instance on a Virtual Host or Cluster Node

Use the `host` argument to specify a virtual host name when starting an Oracle Internet Directory server or Oracle Internet Directory Replication server on a virtual host or a Oracle Application Server Identity Management Cluster Node.

When communicating with the directory server, the directory replication server uses the virtual host name. Further, the `replicaID` attribute that represents the unique replication identification for the Oracle Internet Directory node is generated once. It is independent of the host name and hence requires no special treatment in Oracle Application Server Cold Failover Cluster (Identity Management).

When communicating with the directory server, the Directory Integration Platform server uses the virtual host name.

The following example shows how to start an Oracle Internet Directory server (OIDLDAPD) on a virtual host. The same syntax can be used to also start a directory replication server (OIDREPLD) on a virtual host.

#### Example:

```
oidctl connect=dbs1 host=vhost.company.com server=OIDLDAPD instance=1 \  
configset=2 [flags="..."] start
```

### 2.2.3.9 Reporting the Status of Each Server

The status argument is used to report the status of each server running on the node.

#### Example:

```
oidctl connect=dbs1 status
```

### 2.2.3.10 Reporting Diagnostics

Use the `-diag` flag with the status argument to get detailed diagnostic information that can be useful in resolving performance issues.

The `-diag` flag causes `oidctl` to print information about each LDAP operation as it executes, including the time it spends in the database layer.

For example:

#### **oidctl connect=dbs1 status -diag**

```
oidctl : ORACLE_INSTANCE is not set, defaulting to
/ade/rsathyan_ldmain5/oracle/ldap/
oidctl : INSTANCE_NAME is not set, defaulting to inst1
oidctl : COMPONENT_NAME is not set, defaulting to oid1
+-----+
| Process      | PID   | InstName | CompName | Inst# | Port | Sport |
+-----+
| oidmon       | 12838 | inst1    | oid1     |      |     |      |
+-----+
| oidldapd disp| 12926 | inst1    | oid1     | 1    | 8856 | 0    |
| oidldapd serv| 12930 | inst1    | oid1     | 1    | 8856 | 0    |
| Config DN   | cn=oid1,cn=oslddapd,cn=subconfigsentry
+-----+
+-----+
|Printing LDAP Operation in progress status ...
+-----+
Search:
OIDLDAPD_PID: 12930 WorkerID: 8 DBSID: 162
ConnDN:
BaseDN:c=us
Scope=2
Filter=(|(uid=a*)(cn=b*)(objectclass=person))
ReqdAttrs:
SqlText:
SELECT /*+ FIRST_ROWS */ dn.entryid FROM ct_dn dn WHERE dn.entryi
d IN (SELECT /*+ INDEX( at1 VA_uid ) */ entryid FROM CT_uid at1 W
HERE attrValue like :0 ESCAPE '\' UNION SELECT /*+ INDEX( at1 V
A_cn ) */ entryid FROM CT_cn at1 WHERE attrValue like :1 ESCAPE
'\ ' UNION SELECT /*+ INDEX( at1 VA_objectclass ) */ entryid FROM
CT_objectclass at1 WHERE attrValue = 'person') AND ( (dn.parent
dn like :bdn ESCAPE '\' OR (dn.rdn = :rdn AND dn.parentdn = :pdn
)) ) AND dn.entryid >= :entryThreshold

Plan Hash Value :          0
Rows Fetched      :          0
Number of Sorts  :          0
Disk Read        :          0
Disk Writes      :          0
Buffer Gets      :          0
IO Wait Time     :          0 (ms)
CPU Time         :          0 (ms)
+-----+
```

### 2.2.3.11 Reporting Server Manageability Information

When you run `oidctl` with `status -opdiag interval`, `oidctl` reads the shared memory contents for all servers in the running instances associated with the OIDMON in that environment and aggregates the operation count of each type for each OID component. It repeatedly displays current and total operation counts on the standard output at `interval` seconds. `oidctl` resets all the current values of operation count in the shared memory so that the directory server starts from zero for each type of operation for the next cycle.

For example:

```
$ oidctl status -opdiag 15
oidctl : ORACLE_INSTANCE is not set, defaulting to
/ade/myOID/oracle/ldap/
oidctl : INSTANCE_NAME is not set, defaulting to inst1
oidctl : COMPONENT_NAME is not set, defaulting to oid1

+-----+
+-----+
|Printing completed LDAP operation counts ...
|
+-----+
ComponentName: oid1      Current   Total
      Bind Count      : 0         0
      Add Count       : 0         0
      Delete Count    : 0         0
      Modify Count    : 0         0
      ModRdn Count    : 0         0
      Compare Count   : 0         0
      Search Count    : 0         0
      Extended Count  : 0         0
.
+-----+
+-----+
```

## 2.2.4 Related Command-Line Tools for oidctl

- See [Section 2.4, "oidmon"](#)

## 2.3 oiddiag

The Oracle Internet Directory Server Diagnostic command-line tool (`oiddiag`) collects diagnostic information that helps triage issues reported on Oracle Internet Directory. It is available as `oiddiag` for use on UNIX and Linux platforms and as `oiddiag.bat` for Windows. The tool connects to the database used as the directory store (also called Metadata Repository) of Oracle Internet Directory and reads the information. The tool makes no recommendations on potential fixes to issues. Rather, it collects information to help Support and Development understand a problem and determine its solution. The tool can collect four types of diagnostic information:

- Directory information tree (DIT)
- Data consistency
- Server manageability statistics
- System and process information

If you use either the `collect_all=true` or the `collect_sub=true` arguments, you are prompted to supply the following information:

- The fully domain-qualified database host name
- The database listener port number
- The database service name
- The ODS database user password
- The SYS database user password
- Whether the Oracle Database connection uses SSL or not. Only NoSSL Authentication (Encryption only) is supported.

You can find the host name, port number and service name in the file `tnsnames.ora`, located by default in `ORACLE_INSTANCE/config`. For example, in the following `tnsnames.ora` file, the hostname, port number and service names are, respectively, `sun16.example.com`, `1521`, and `orcl.example.com`:

```
ORCL =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP)(HOST = sun16.example.com)(PORT = 1521))
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SERVICE_NAME = orcl.example.com)
    )
  )
```

---

---

**Note:** You must set the `ORACLE_HOME` environment variable before executing the `OIDDIA` tool.

---

---

### 2.3.1 Syntax for oiddiag

```
oiddiag {listdiags=true [targetfile=filename]} | {collect_all=true
[outfile=filename]} | {collect_sub=true [infile=filename] [outfile=filename]} |
{audit_report=true [outfile=file_name]}
```

### 2.3.2 Arguments for oiddiag

#### **listdiags=true**

Writes a list of available diagnostics that can be collected. The list is written to an output file, which is `ORACLE_INSTANCE/diagnostics/logs/OID/tools/oiddiag.txt` by default. You should run a `listdiags` command before running a `collect_sub` command. The `collect_sub` command uses the file that is output by `listdiags`. You can edit this file as needed to contain only the diagnostic items you want.

#### **targetfile=filename**

This is the location of the output file where the diagnostic tool writes the list of available diagnostics when `listdiags=true` is given. If not specified, the tool writes the list to `ORACLE_INSTANCE/diagnostics/logs/OID/tools/oiddiag.txt`.

#### **collect\_all=true**

Collect all of the diagnostic information available and writes it to an output file. You are prompted to provide the Oracle Internet Directory database host name, listener port, net service name, and password.



**outfile=filename**

The name of the output file that the diagnostic information is written to. If not specified, the default output file is written to `ORACLE_INSTANCE/diagnostics/logs/OID/tools/oiddiag/timestamp.log`. The timestamp format is `YYYYMMDDHHmmss`.

**collect\_sub=true**

Collects a subset of diagnostic information (based on the diagnostics specified in the input file) and writes it to an output file. You are prompted to provide the Oracle Internet Directory database host name, listener port, net service name, and password.

You should run a `listdiags` command before running a `collect_sub` command. The `collect_sub` command uses the file that is output by `listdiags`. You can edit this file as needed to contain only the diagnostic items you want.

**infile=filename**

A file that contains the list of diagnostic items for which you want to output information. By default, the diagnostic tool looks for this file in `ORACLE_INSTANCE/diagnostics/logs/OID/tools/oiddiag.txt`, which is the default target file location of the `listdiags` command. You can edit this file as needed to contain only the diagnostic items you want.

**audit\_report=true**

Generates standard reports for Secure Events Tracking and writes them to an output file.

### 2.3.3 Tasks and Examples for oiddiag

Using the Oracle Internet Directory diagnostic tool, you can perform the following tasks:

- [Section 2.3.3.1, "Collecting All Diagnostic Information"](#)
- [Section 2.3.3.2, "Collecting Selected Diagnostic Information"](#)
- [Section 2.3.3.3, "Collecting Stack Trace Information"](#)

#### 2.3.3.1 Collecting All Diagnostic Information

The following example shows how to collect all available diagnostic information and write it to the specified output file.

**Example:**

```
oiddiag collect_all=true outfile=~ /myfiles/oid.log
```

#### 2.3.3.2 Collecting Selected Diagnostic Information

To collect a subset of diagnostic data, you must first run the `oiddiag` tool with the `listdiags` argument. This outputs a list of available diagnostics, which you can then edit. This list is then passed in to the `collect_sub` command to determine the diagnostics for which to collect output. The following example uses the default file locations of `ORACLE_INSTANCE/diagnostics/logs/OID/tools/oiddiag.txt` (for the list) and `ORACLE_INSTANCE/diagnostics/logs/OID/tools/oiddiagtimestamp.log` (for the output file).

**Example:**

```
oiddiag listdiags=true
oiddiag collect_sub=true
```

**2.3.3.3 Collecting Stack Trace Information**

An important type of information that the `oiddiag` tool collects is the stack trace data for Oracle Internet Directory processes. Examining the stack trace is useful if you are experiencing slow response times or if your system stops responding. Because Oracle Internet Directory is usually started as a `setuid-root` program, you must log in as the root user before you can use the `oiddiag` tool to trace the stack for any Oracle Internet Directory processes. The root user must belong to the same operating system group that the Oracle operating system user belongs to. The following example logs in as the root user and changes to the `dba` group before executing the `oiddiag` tool:

```
su
newgrp dba
oiddiag collect_all=true
```

## 2.4 oidmon

In 11g Release 1 (11.1.1), you typically manage Oracle Internet Directory by using Oracle Enterprise Manager Fusion Middleware Control or the command-line utility `opmnctl`. Both `opmnctl` and Fusion Middleware Control use the Oracle Process Manager and Notification Server to issue commands to the Oracle Internet Directory Monitor, `oidmon`, which initiates, monitors, and terminates directory server processes.

### 2.4.1 Syntax for oidmon

```
oidmon [connect=connect_string] [host=hostname] [sleep=seconds] start | stop
```

### 2.4.2 Arguments for oidmon

**connect=connect\_string**

Required. The directory database connect string. If you already have a `tnsnames.ora` file configured, then this is the net service name specified in that file, which is located by default in `ORACLE_INSTANCE/config`. (You can set the `TNS_ADMIN` environment variable if you want to use a different location.)

**host=hostname**

Optional. Enables you to specify a virtual host name for the server or the name of an Oracle Application Server Identity Management Cluster Node. If not given, the default of `localhost` is used.

**sleep=seconds**

Optional. The number of seconds after which Oracle Internet Directory Monitor should check for new requests from Oracle Internet Directory Control and for requests to restart any server instances that may have stopped. The default is 10 seconds.

**start | stop**

Required. The operation to perform (start or stop the Monitor process).

## 2.4.3 Tasks and Examples for oidmon

Using Oracle Internet Directory Monitor, you can perform the following tasks:

- [Section 2.4.3.1, "Starting Oracle Internet Directory Monitor"](#)
- [Section 2.4.3.2, "Starting Oracle Internet Directory Monitor on a Virtual Host or Cluster Node"](#)
- [Section 2.4.3.3, "Stopping Oracle Internet Directory Monitor"](#)

### 2.4.3.1 Starting Oracle Internet Directory Monitor

You should start Oracle Internet Directory Monitor before using Oracle Internet Directory Control.

**Example:**

```
oidmon connect=dbs1 sleep=15 start
```

### 2.4.3.2 Starting Oracle Internet Directory Monitor on a Virtual Host or Cluster Node

Use the `host` argument to specify a virtual host name when starting an Oracle Internet Directory Monitor on a virtual host or a Oracle Application Server Identity Management Cluster Node.

**Example:**

```
oidmon connect=dbs1 host=virtualhostname.company.com start
```

### 2.4.3.3 Stopping Oracle Internet Directory Monitor

Stopping Oracle Internet Directory Monitor also stops all other Oracle Internet Directory processes. The `oidmon` tool does not remove server instance information from the `ODS_PROCESS` table. When an `oidmon start` operation is executed, it starts all the server processes it had stopped previously.

**Example:**

```
oidmon connect=dbs1 stop
```

## 2.4.4 Related Command-Line Tools for oidmon

- See [Section 2.2, "oidctl"](#)

## 2.5 opmnctl

The Oracle Process Manager and Notification Server Control Utility (`opmnctl`) enables you to manage system components, such as Oracle Internet Directory, in an integrated way.

The term "instance" refers to an Oracle instance in `opmnctl` command descriptions.

---

**Notes:**

- This section only discusses how to use the OPMN Control Utility to manage Oracle Internet Directory components. For detailed information on how to use the OPMN Control Utility, see *Oracle Fusion Middleware Oracle Process Manager and Notification Server Administrator's Guide*.
  - Arguments to `opmnctl` are case-sensitive. Be sure to type them exactly as shown. For example, `-adminUsername` must have only the letter U in upper case.
- 

## 2.5.1 Syntax for `opmnctl`

```
opmnctl startproc ias-component=componentName

opmnctl stopproc ias-component=componentName

opmnctl restartproc ias-component=componentName

opmnctl restartproc process-type=componentType

opmnctl createcomponent [admin_server_properties] [instance_properties]
[opmn_properties] [component_properties] [component_configuration_properties]

opmnctl deletecomponent [admin_server_properties] [instance_properties]
[opmn_properties] [component_properties] [component_configuration_properties]

opmnctl registerinstance [admin_server_properties] [instance_properties]
[component_configuration_properties]

opmnctl unregisterinstance [admin_server_properties] [instance_properties]
[component_configuration_properties]

opmnctl updatecomponentregistration [admin_server_properties]
[instance_properties] [component_configuration_properties]

opmnctl status [-l]
```

## 2.5.2 Arguments for `opmnctl`

Arguments for `opmnctl` consist of commands and several types of properties. This section describes the following types of arguments:

- [Section 2.5.2.1, "Commands"](#)
- [Section 2.5.2.2, "WebLogic Administration Server Properties"](#)
- [Section 2.5.2.3, "Instance Properties"](#)
- [Section 2.5.2.4, "OPMN Configuration Properties"](#)
- [Section 2.5.2.5, "Component Properties for Oracle Internet Directory"](#)
- [Section 2.5.2.6, "Oracle Internet Directory Component Configuration Properties"](#)

---

---

**Note:** Arguments to `opmnctl` are case-sensitive. Be sure to type them exactly as shown. For example, `-adminUsername` must have only the letter `U` in upper case.

---

---

### 2.5.2.1 Commands

The command indicates the operation to perform. The following commands are relevant to Oracle Internet Directory:

#### **startproc**

Starts server process.

#### **stopproc**

Stops server process.

#### **restartproc**

Restarts a specific Oracle Internet Directory component or all Oracle Internet Directory components.

#### **createcomponent**

Creates a component and automatically registers the component with a WebLogic domain, as long as the instance is in a registered state.

#### **deletecomponent**

Deletes a component.

#### **registerinstance**

Registers an Oracle instance that was not previously registered with a domain. This scenario occurs if you chose **Configure Without a Domain** during installation of Oracle Internet Directory or if you created an Oracle instance from the command line and did not register the instance.

#### **unregisterinstance**

Unregisters an Oracle instance that was previously registered with a domain.

#### **status [-l]**

Shows the status of components. Add the `-l` option for detailed information.

#### **updatecomponentregistration**

Registers an existing Oracle Internet Directory component that was not previously registered with a domain. This scenario occurs if you created a new component in an Oracle instance using `opmnctl createcomponent` and did not register the component.

### 2.5.2.2 WebLogic Administration Server Properties

The following administration server properties are relevant to Oracle Internet Directory:

#### **-adminHost**

The WebLogic Administration Server host name

**-adminPort**

The WebLogic Administration Server port. The default is 7001.

**-adminUsername**

The WebLogic administrator user name.

**-adminPasswordFile**

A text file containing the WebLogic administrator password. You are prompted for the administrator password if this parameter is missing. Best security practice is to provide the password in response to a prompt. If you must use a file containing the password in clear text, protect it with file permissions and delete it when it is no longer needed.

**2.5.2.3 Instance Properties**

You do not need to specify instance properties with the `opmnctl` command, as long as you invoke the command as `ORACLE_INSTANCE/bin/opmnctl`.

**2.5.2.4 OPMN Configuration Properties**

No OPMN configuration properties are required with the `opmnctl` commands shown in this chapter.

**2.5.2.5 Component Properties for Oracle Internet Directory**

The following component properties are relevant to Oracle Internet Directory.

**-componentType**

For Oracle Internet Directory, this is always `OID`. This is required for `createcomponent`.

**-componentName**

The name of an Oracle Internet Directory component, such as `oid1`. The component name must be unique within the Oracle instance.

**2.5.2.6 Oracle Internet Directory Component Configuration Properties**

These arguments are specific to Oracle Internet Directory

**-Db\_info**

Specifies the name, TNS port, and service name of the Oracle Database associated with this Oracle Internet Directory component, in the format:

```
DBHostName:TNSPORT:DBSERVICENAME
```

For example:

```
linux12.example.com:1521:orcl.example.com
```

When you are using the `createcomponent` command, the `DBHostName:Port:DBSvcName` argument to the `-DB_info` parameter must be the same as that provided during installation. If it is not, the command fails. You can find this value in the file `ORACLE_INSTANCE/config/tnsnames_copy.ora`.

If the Oracle Database is based on Real Application Clusters, the argument to the `-DB_info` parameter is of the form:

```
DBHostName1:Port1^DBHostName2:Port2@DBSvcName
```

**-Ods\_Password\_File**

Optional. The file that contains the ODS password in cleartext. You are prompted for the ODS password if this parameter is missing. Best security practice is to provide the password in response to a prompt. If you must use a file containing the password in clear text, protect it with file permissions and delete it when it is no longer needed.

**-Sm\_Password\_File**

Optional. The file that contains the ODSSM password in cleartext. You are prompted for the ODSSM password if this parameter is missing. Best security practice is to provide the password in response to a prompt. If you must use a file containing the password in clear text, protect it with file permissions and delete it when it is no longer needed.

**-Namespace**

Required only for the first Oracle Internet Directory component in an instance. The Oracle Internet Directory namespace. For example: "dc=us,dc=example,dc=com".

**-Admin\_Password\_File**

Optional. The file that contains the password for the Oracle Internet Directory superuser account `cn=orcladmin`. You are prompted for the Oracle Internet Directory superuser password if this parameter is missing.

**-Port**

Optional. The non-SSL port for this Oracle Internet Directory component. The command uses a default available port if this parameter is missing.

**-Sport**

Optional. The SSL port for this Oracle Internet Directory component. The command uses a default available port if this parameter is missing.

### 2.5.3 Tasks and Examples for opmnctl

Using the OPMN Control Utility, you can perform the following Oracle Internet Directory server management tasks:

- [Section 2.5.3.1, "Creating an Oracle Internet Directory Component"](#)
- [Section 2.5.3.2, "Registering an Oracle Instance"](#)
- [Section 2.5.3.3, "Unregistering an Oracle Instance"](#)
- [Section 2.5.3.4, "Updating the Component Registration of an Oracle Instance"](#)
- [Section 2.5.3.5, "Deleting an Oracle Internet Directory Component"](#)
- [Section 2.5.3.6, "Stopping All Oracle Internet Directory Server Components"](#)
- [Section 2.5.3.7, "Starting All Oracle Internet Directory Server Components"](#)
- [Section 2.5.3.8, "Stopping a Specific Oracle Internet Directory Server Component"](#)
- [Section 2.5.3.9, "Starting a Specific Oracle Internet Directory Server Component"](#)
- [Section 2.5.3.10, "Restarting All Oracle Internet Directory Server Components"](#)
- [Section 2.5.3.11, "Restarting a Specific Oracle Internet Directory Server Component"](#)
- [Section 2.5.3.12, "Getting Status Information"](#)

### 2.5.3.1 Creating an Oracle Internet Directory Component

This command creates a component and registers it with a WebLogic domain, as long as the instance is in a registered state:

```
opmnctl createcomponent
  -componentType OID
  -componentName oid2
  -adminHost myhost
  -adminPort 7001
  -DB_info "linux12.example.com:1521:orcl.example.com"
  -Namespace "dc=domain_component1,dc=domain_component2..."
```

The *DBHostName:Port:DBSvcName* argument to the `-DB_info` parameter must be the same as that provided during installation. If it is not, the command fails. You can find this value in the file `ORACLE_INSTANCE/config/tnsnames_copy.ora`

If the Oracle Database is based on Real Application Clusters, the argument to the `-DB_info` parameter is of the form:

```
DBHostName1:Port1^DBHostName2:Port2@DBSvcName
```

The `opmnctl` command prompts for the WebLogic administrator's user name if you do not supply it. It also prompts for the passwords if you do not supply password file names on the command line. The `opmnctl` command also uses available ports if you do not specify `-Port` or `-Sport`

### 2.5.3.2 Registering an Oracle Instance

This example registers an Oracle instance with a WebLogic server:

```
ORACLE_INSTANCE/bin/opmnctl registerinstance \
  -adminHost myhost \
  -adminPort 7001 \
  -adminUsername weblogic
```

You are prompted for the WebLogic administrator's user name and password.

### 2.5.3.3 Unregistering an Oracle Instance

This example unregisters an Oracle instance with a WebLogic server:

```
ORACLE_INSTANCE/bin/opmnctl unregisterinstance \
  -adminHost myhost \
  -adminPort 7001 \
  -adminUsername weblogic
```

You are prompted for the WebLogic administrator's user name and password if you do not supply them.

### 2.5.3.4 Updating the Component Registration of an Oracle Instance

You must update the registration of an Oracle Internet Directory component in a registered Oracle instance whenever you change any of the configuration attributes `orclhostname`, `orclsslport`, or `orclnonsslport` in the instance-specific configuration entry, or if you change the password for the EMD administrator. If you do not update the component registration, you will be unable to use Fusion Middleware Control or `wlst` to manage that component.

This example updates the component registration of an Oracle instance that has been registered.

```
ORACLE_INSTANCE/bin/opmnctl updatecomponentregistration \
```



```

-adminHost myhost \
-adminPort 7001 \
-adminUsername weblogic
-componentType OID \
-componentName oid2 \
-Port 6589 \
-Sport 3032

```

You are prompted for the WebLogic administrator's user name and password if you do not supply them.

The default administrative port on the WebLogic Administration Server is 7001.

You must supply both a non-SSL port and an SSL port.

### 2.5.3.5 Deleting an Oracle Internet Directory Component

This example deletes an Oracle Internet Directory component that has been registered with a WebLogic server:

```

ORACLE_INSTANCE/bin/opmnctl deletecomponent \
-adminHost myhost \
-adminPort 7001 \
-adminUsername weblogic \
-componentType OID \
-componentName oid2

```

You are prompted for the WebLogic administrator's user name and password if you do not supply them.

### 2.5.3.6 Stopping All Oracle Internet Directory Server Components

The following example shows how to stop all running directory server processes (Oracle Internet Directory and Oracle Directory Replication server).

```

ORACLE_INSTANCE/bin/opmnctl process-type=OID stop

```

### 2.5.3.7 Starting All Oracle Internet Directory Server Components

The following example shows how to start all directory server components.

```

$ORACLE_INSTANCE/bin/opmnctl startproc componentType=OID

```

### 2.5.3.8 Stopping a Specific Oracle Internet Directory Server Component

The following example shows how to stop a specific Oracle Internet Directory component.

```

ORACLE_INSTANCE/bin/opmnctl stopproc componentName=oid1

```

### 2.5.3.9 Starting a Specific Oracle Internet Directory Server Component

The following example shows how to start a specific Oracle Internet Directory component.

```

ORACLE_INSTANCE/bin/opmnctl startproc componentName=oid1

```

### 2.5.3.10 Restarting All Oracle Internet Directory Server Components

The following example shows how to restart all Oracle Internet Directory components.

```
ORACLE_INSTANCE/bin/opmnctl restartproc process-type=OID
```

### 2.5.3.11 Restarting a Specific Oracle Internet Directory Server Component

The following example shows how to restart an Oracle Internet Directory component named oid1.

```
ORACLE_INSTANCE/bin/opmnctl restartproc ias-component=oid1
```

### 2.5.3.12 Getting Status Information

The following example shows the status information provided by opmnctl.

```
$ opmnctl status -l
```

```
Processes in Instance: asinst_2
```

```
-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+
ias-component          | process-type   | pid | status | uid | memused
| uptime | ports
+-----+-----+-----+-----+-----+-----+
oid2                   | oidldapd      | 24760 | Alive  | 988238800 | 102744
| 0:01:12 | N/A
oid2                   | oidldapd      | 24756 | Alive  | 988238799 | 55052
| 0:01:12 | N/A
oid2                   | oidmon        | 24745 | Alive  | 988238796 | 48168
| 0:01:14 | LDAPS:6789,LDAP:6788

oid1                   | oidldapd      | 21590 | Alive  | 988238048 | 103716
| 19:51:48 | N/A
oid1                   | oidldapd      | 21586 | Alive  | 988238047 | 54420
| 19:51:49 | N/A
oid1                   | oidmon        | 21577 | Alive  | 988238046 | 48168
| 19:51:49 | LDAPS:3133,LDAP:3060
```

## 2.5.4 Related Command-Line Tools for opmnctl

- See [Section 2.4, "oidmon"](#)
- See [Section 2.2, "oidctl"](#)

## 2.6 oidstats.sql

Use the Oracle Internet Directory Database Statistics Collection Tool (`oidstats.sql`) to analyze the various database `ods` (Oracle Directory Server) schema objects to estimate the statistics. It is located in the following directory: `ORACLE_HOME/ldap/admin/`. You must run this utility whenever there are significant changes in directory data—including the initial load of data into the directory.

If you load data into the directory by any means other than the bulk load tool (`bulkload`), then you must run the Oracle Internet Directory Database Statistics Collection tool after loading. Statistics collection is essential for the Oracle Optimizer to choose an optimal plan in executing the queries corresponding to the LDAP operations. You can run Oracle Internet Directory Database Statistics Collection tool at any time, without shutting down any of the Oracle Internet Directory processes.

---



---

**Note:** If you do not use the bulkload utility to populate the directory, then you must run the `oidstats.sql` tool to avoid significant search performance degradation.

---



---

## 2.6.1 Syntax for `oidstats.sql`

```
sqlplus ods/ods_password@connect_string @oidstats.sql
```

## 2.6.2 Arguments for `oidstats.sql`

If you do not supply the ODS password on the command line, `sqlplus` prompts for it. Note that the default ODS password is the same as that for the Oracle Application Server administrator. (For security reasons, avoid supplying a password on the command line whenever possible. A password typed on the command line is visible on your screen. When you supply a password at a prompt, it is not visible on the screen.)

### **connect\_string**

Required. The connect string for the ODS database. This is the network service name set in the `tnsnames.ora` file, which is located by default in `$ORACLE_INSTANCE/config`. (You can set the `TNS_ADMIN` environment variable if you want to use a different location.)

## 2.6.3 Tasks and Examples for `oidstats.sql`

You can perform the following task using the `oidstats.sql` tool:

- [Section 2.6.3.1, "Running the Oracle Internet Directory Database Statistics Collection Tool"](#)

### 2.6.3.1 Running the Oracle Internet Directory Database Statistics Collection Tool

#### **Example:**

```
sqlplus ods@dbs1 @oidstats.sql
```

## 2.6.4 Related Command-Line Tools for `oidstats.sql`

- See [Section 3.2, "bulkload"](#).

## 2.7 oidcred

The Oracle Internet Directory Credential Management Tool is used to add, update, or delete a credential that has been created in the Credential Store Framework. It determines the instance name from the `opmn.xml` file

### 2.7.1 Syntax for `oidcred`

```
oidcred user_name option [InstancePath]
```

### 2.7.2 Arguments for `oidcred`

The `oidcred` command takes the following arguments:

**user\_name**

Required. Value can be odssm or emd.

**option**

Required. Value can be update or delete. The update option adds the credential if it does not exist or updates it if it exists.

**InstancePath**

Required if ORACLE\_INSTANCE environment is not set. Path of Oracle Instance directory.

If not specified on the command line, oidcred uses ORACLE\_INSTANCE environment variable if set.

## 2.7.3 Tasks and Examples for oidcred

Update the password for user odssm in the Credential Store Framework.

```
oidcred odssm update /scratch/mydir/fmw_home/asinst_1
Enter password:
Confirm password:
Password set in CSF
```

## 2.8 oidrealm

The Oracle Internet Directory realm tool is used to create multiple realms in Oracle Internet Directory. The individual realms can be managed separately, so you can use oidrealm as a replacement for Delegated Administration Services.

The oidrealm tool supports creation, but not deletion, of a realm. A procedure for deleting a realm is provided in Note 604884.1, which is available on My Oracle Support at <https://support.oracle.com/>

### 2.8.1 Syntax for oidrealm

On UNIX or Linux:

```
oidrealm oid_host oid_port DN [-SSL]
```

On Windows:

```
oidrealm.bat oid_host oid_port DN [-SSL]
```

---

---

**Note:** If you specify an SSL port, that port must be configured in SSL No Authentication Mode, that is, orclsslauthentication must be 1. For more information, see the section on SSL authentication modes in *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*.

---

---

### 2.8.2 Arguments for oidrealm

**oid\_host**

Name of host where Oracle Internet Directory is running.

**oid\_port**

Specifies the port number to use, which can be either SSL or non-SSL

**DN**

DN of realm to add

**[-SSL]**

Specifies that the port is an SSL port. Only no-auth mode is supported.

**2.8.3 Example for oidrealm**

```
$ oidrealm myhost.example.com 3133 'dc=newrealm,dc=com' -SSL
Enter OID Admin Password: password

[info] ->>
/scratch/mydir/mwhome/idm3/ldap/schema/oid/oidSubscriberCreateCommon.lst *
Feb 2, 2009 9:22:57 PM oracle.ldap.util.LDIFLoader recursiveLoad
INFO: ->> /scratch/mydir/mwhome/idm3/ldap/schema/oid/oidSubscriberCreateCommon.lst
*
[info] ->> /scratch/mydir/mwhome/idm3/ldap/schema/oid/oidContextCreate.lst *
Feb 2, 2009 9:22:57 PM oracle.ldap.util.LDIFLoader recursiveLoad
INFO: ->> /scratch/mydir/mwhome/idm3/ldap/schema/oid/oidContextCreate.lst *
[info] -> LOADING:
/scratch/mydir/mwhome/idm3/ldap/schema/oid/oidContextCreateCommon.sbs
Feb 2, 2009 9:22:57 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING:
/scratch/mydir/mwhome/idm3/ldap/schema/oid/oidContextCreateCommon.sbs
[info] ->>
/scratch/mydir/mwhome/idm3/ldap/schema/oid/oidContextUpgradeFrom81600.lst *Feb 2,
2009 9:22:58 PM oracle.ldap.util.LDIFLoader recursiveLoad
INFO: ->>
/scratch/mydir/mwhome/idm3/ldap/schema/oid/oidContextUpgradeFrom81600.lst*
[info] -> LOADING:
/scratch/mydir/mwhome/idm3/ldap/schema/oid/oidContextUpgradeFrom81600Common.sbs
Feb 2, 2009 9:22:58 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING:
/scratch/mydir/mwhome/idm3/ldap/schema/oid/oidContextUpgradeFrom81600Common.sbs
[info] ->>
/scratch/mydir/mwhome/idm3/ldap/schema/oid/oidContextCreate90100Changes.lst *
Feb 2, 2009 9:23:00 PM oracle.ldap.util.LDIFLoader recursiveLoad
INFO: ->>
/scratch/mydir/mwhome/idm3/ldap/schema/oid/oidContextCreate90100Changes.lst *
[info] -> LOADING:
/scratch/mydir/mwhome/idm3/ldap/schema/oid/oidContextUpgradeFrom90000Common.sbs
Feb 2, 2009 9:23:00 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
...
...
...
...
```



---

---

# Oracle Internet Directory Data Management Tools

This chapter describes the data management command-line tools used to administer the entries and data stored in Oracle Internet Directory.

This chapter includes the following sections:

- Section 3.1, "bulkdelete"
- Section 3.2, "bulkload"
- Section 3.3, "bulkmodify"
- Section 3.4, "catalog"
- Section 3.5, "ldapadd" (LDAP Data Add Tool)
- Section 3.6, "ldapaddmt" (Multi-Threaded LDAP Data Add Tool)
- Section 3.7, "ldapbind" (Authentication Validation Tool)
- Section 3.8, "ldapcompare" (Attribute Comparison Tool)
- Section 3.9, "ldapdelete" (LDAP Data Deletion Tool)
- Section 3.10, "ldapmoddn" (LDAP DN/RDN Modification Tool)
- Section 3.11, "ldapmodify" (LDAP Data Modification Tool)
- Section 3.12, "ldapmodifymt" (Multi-Threaded LDAP Data Modification Tool)
- Section 3.13, "ldapsearch" (LDAP Search Tool)
- Section 3.14, "ldifmigrator" (Data Migration Tool)
- Section 3.15, "ldifwrite" (Data Export Tool)
- Section 3.16, "upgradecert.pl" (Certificate Upgrade Tool)

---

---

**Notes:**

- The bulk tools do not support attribute uniqueness.
  - If your schema were created during installation of a version prior to 11g Release 1 (11.1.1.6.0), you must add data files to the OLTS\_CT\_STORE and OLTS\_ATTRSTORE tablespaces if you intend to add more than a million entries to Oracle Internet Directory. Perform this step prior to the bulkload or ldapadd operation. For details, see the section "*Creating Datafiles and Adding Datafiles to a Tablespace*" in *Oracle Database Administrator's Guide*.
- 
-

## 3.1 bulkdelete

The `bulkdelete` command-line tool enables you to delete one or more subtrees efficiently. It can be used when both an Oracle Internet Directory server and Oracle Directory Replication servers are in operation. It uses a SQL interface to benefit performance. For this release, the `bulkdelete` tool runs on only one node at a time.

This tool does not support filter-based deletion. That is, it deletes an entire subtree below the root of the subtree. If the base DN is a user-added DN, rather than a DN created as part of the installation of the directory, it is included in the delete. You must restrict LDAP activity against the subtree during deletion.

---

---

**Note:** The `bulkdelete` command requires that the environment variable `ORACLE_INSTANCE` be set.

---

---

### 3.1.1 Syntax for bulkdelete

```
bulkdelete connect=connect_string {[basedn=Base_DN] | [file=file_name]}
[cleandb="TRUE" | "FALSE"] [size=transaction_size] [encode=character_set]
[debug="TRUE" | "FALSE"] [threads=num_of_threads] [verbose="TRUE" | "FALSE"]
```

### 3.1.2 Arguments for bulkdelete

#### **connect**

Required. The directory database connect string. If you already have a `tnsnames.ora` file configured, then this is the net service name specified in that file, which is located by default in `ORACLE_INSTANCE/config`. (You can set the `TNS_ADMIN` environment variable if you want to use a different location.)

#### **basedn | file**

Required. The base DN of the subtree to be deleted, for example, `"dc=company, dc=com"`. Enclose the DN in quotation marks. You can also specify multiple base DN's by putting them in a file and specifying the file name and path with the `file` argument.

#### **cleandb**

Optional. This is used to specify whether the deleted entries would be tombstoned or deleted completely from the database. The default (`cleandb="TRUE"`) is to delete the entries completely.

#### **size**

Optional. The number of entries to be committed as a part of one transaction.

#### **encode**

Optional. The native character set encoding. Defaults to the character set of the user's terminal. Each supported character set has a unique acronym, for example, `WE8MSWIN1252`, `JA16SJIS`, or `AL32UTF8`.

#### **debug**

Optional. The `debug` option reports the logging level. This is useful in case the command runs into errors. The output is logged to the `bulkdelete.log` file. This file can be found under `ORACLE_INSTANCE/diagnostics/logs/OID/tools`.



**threads**

Optional. The number of threads to create. The default value is the number of CPUs on the machine plus one.

**verbose**

Optional. This is used to run the command in verbose mode.

### 3.1.3 Tasks and Examples for bulkdelete

The following examples show how to delete one or more subtrees from the directory:

- [Section 3.1.3.1, "Deleting All Entries in a Naming Context and Making Them Tombstone Entries"](#)
- [Section 3.1.3.2, "Completely Deleting All Entries in a Naming Context"](#)
- [Section 3.1.3.3, "Deleting Entries in Multiple Naming Contexts"](#)

#### 3.1.3.1 Deleting All Entries in a Naming Context and Making Them Tombstone Entries

**Example:**

```
bulkdelete connect="dbs1" basedn="cn=OracleContext" cleandb="FALSE"
```

#### 3.1.3.2 Completely Deleting All Entries in a Naming Context

**Example:**

```
bulkdelete connect="dbs1" basedn="cn=OracleContext"
```

#### 3.1.3.3 Deleting Entries in Multiple Naming Contexts

This example uses a file that contains a list of DNs to delete.

**Example:**

```
bulkdelete connect="dbs1" file="~/myfiles/dn.txt"
```

### 3.1.4 Related Command-Line Tools for bulkdelete

- See [Section 3.2, "bulkload"](#)
- See [Section 3.3, "bulkmodify"](#)
- See [Section 3.9, "ldapdelete"](#)

## 3.2 bulkload

The `bulkload` command-line tool is useful for loading large number of entries into a directory server. It uses Oracle SQL\*Loader to load the directory entries. The `bulkload` tool expects the input file to be in LDAP Data Interchange Format (LDIF). See [Appendix A, "LDIF File Format"](#) for the correct format and syntax of an LDIF file.

Intermediate files used by `bulkload` are stored in `ORACLE_INSTANCE/OID/load` by default.

---

---

**Note:** The `bulkload` command requires that the environment variable `ORACLE_INSTANCE` be set.

---

---

### Using bulkload with Replication

When you add data to a node that is part of a Directory Replication Group (DRG), you can use either bulk tools or LDAP tools, depending on the circumstances. The following rules apply:

- When you add new entries to all nodes in the DRG, you can use either bulk tools or LDAP tools. For more than 20K entries, bulk tools are significantly faster. If you use LDAP tools, add the entries to only one node in the DRG and let replication propagate the entries. If you use bulk tools, generate the intermediate file only once from the LDIF file and use that intermediate file to load the entries onto all the nodes in the DRG.
- When you copy existing entries from one node to another in the same replication group, use bulk tools. Use the `bulkload` option `restore=true` when you upload the data.
- If the LDIF file contains operational attributes, which it does when created with `ldifwrite`, use `bulkload` to add the entries.
- If the replication agreement is a partial replication agreement, use `ldifwrite` with the base DN as the replication agreement DN to write the entries to the LDIF file. Then use `bulkload` with the `restore=true` option to load the data.

### Overview of the Bulk Loading Tool Operations

The Bulk Loading Tool performs its operations in the following phases:

#### 1. Check

In the check phase, all entries of LDIF files are verified for valid LDAP schema and duplicate entries. The Bulk Loading Tool reports any errors, which must be corrected before proceeding.

#### 2. Generate

In the generate phase, the LDIF input is converted into intermediate files that can be used by `SQL*Loader` to load the data into the Oracle Internet Directory directory store.

#### 3. Load

The Intermediate files generated in generate phase are loaded into the Oracle Internet Directory directory store. The Bulk Loading Tool supports two types of loading of data:

- **Incremental Mode Loading**

Incremental mode enables you to append data to existing directory data. Loading in this mode is faster than other add methods, but slower than bulk mode loading.

Use this mode when you want to append a small amount of data. Here, small amount is a relative number. It depends upon existing data in directory, the amount of data to be loaded, and the hardware capabilities to handle the load.

In this mode, the Bulk Loading Tool does not drop and rebuild catalog indexes. Instead, it uses `SQL*Loader` in insert mode to add data to the database and update indexes through inserts.

### ■ Bulk Mode Loading

In bulk mode, you must be able to add or append large number of entries to a directory. By default, the Bulk Loading Tool runs in bulk mode. Bulk mode is faster than incremental mode.

In bulk mode, all Oracle Internet Directory server instances should be stopped. In this mode, the Bulk Loading Tool drops existing indexes and re-creates them after loading of data. For data loading, it uses SQL\*Loader direct-path mode.

---



---

#### Notes:

- Running the `bulkload -load` operation sets the server mode to read-write. If you require a different mode, reset it after performing the load operation.
- At the start of the load operation, `bulkload` determines the current configured value of `orclRIenabled`, then disables referential integrity. At the end of load phase, `bulkload` returns `orclRIenabled` to its original value. If any referential integrity violations occurred, however, referential integrity is disabled, and you see the message:

```
There is a violation of Referential Integrity and hence it is
Disabled now. Run the OIDDIAG tool with diagnostic option to
collect the Entries which have dangling DN attribute values and
Fix the violation
Fix the violation and then set orclRIenabled to the desired value.
```

---



---

#### 4. Index Creation

After the load is complete, the indexes are re-created if the load was done in bulk mode. Also, the Bulk Loading Tool provides an option just to re-create all indexes. This is useful in case if previous index creation was unsuccessful for some reason.

#### 5. Directory Data Recovery

A failure in the load phase can leave directory data in an inconsistent state. The Bulk Loading Tool can revert back to original state that existed prior to the invocation of `bulkload`.

#### Before Using the bulkload Tool

Before running the `bulkload` tool:

1. Stop your Oracle Internet Directory server instance(s) before loading data in bulk mode.
2. Take a cold backup of the Oracle Internet Directory database.
3. If loading data in incremental mode, you do not need to stop the directory server, although you must put the directory server in read-modify mode. Read-modify mode restricts add, delete, and modify DN operations.
4. If loading an LDIF file with data from an older version of Oracle Internet Directory, see the *Oracle Fusion Middleware Upgrade Planning Guide* for any special instructions about upgrading `orclguids` before you begin.

### 3.2.1 Syntax for bulkload

```
bulkload [connect=connect_string]
{[check="TRUE"|"FALSE" [file=ldif_file]] [generate="TRUE"|"FALSE"
[append="TRUE"|"FALSE"] [restore="TRUE"|"FALSE"] [thread=num_of_threads]
file=ldif_file]
[load="TRUE"|"FALSE" [append="TRUE"|"FALSE"] [threads=num_of_threads]]
[index="TRUE"|"FALSE"] [missing="TRUE"|"FALSE"] [recover="TRUE"|"FALSE"]}
[encode=character_set] [debug="TRUE"|"FALSE"] [verbose="TRUE"|"FALSE"]
```

### 3.2.2 Arguments for bulkload

#### connect

Optional. The directory database connect string. If you already have a `tnsnames.ora` file configured, then this is the net service name specified in that file, which is located by default in `ORACLE_INSTANCE/config`. (You can set the `TNS_ADMIN` environment variable if you want to use a different location.) For loading data in single node, specify its connect string—for example `orcl`. For loading data in multiple nodes, specify connect strings of all nodes—for example:

```
bulkload connect="orcl1,orcl2,orcl3"
```

#### check | generate | load | recover | index | missing

Required. The operation to perform. The operations are:

- `check` - Checks the LDIF file provided for schema inconsistencies and for duplicate entry DNs. You must provide the full path or relative path and file name of an LDIF file. You can optionally specify the number of threads. The `check` and `generate` operations can be issued at the same time.
- `generate` - Creates intermediate files suitable for loading entries into Oracle Internet Directory using SQL\*Loader. You must provide the full path or relative path and file name of an LDIF file from which to generate entries. You can optionally specify the number of threads. The `check` and `generate` operations can be issued at the same time.

---



---

#### Note:

After the `generate` operation, the directory is left in the read-modify mode until you perform the `load` operation.

`bulkload` updates the mode to read-only when performing a load operation.

---



---

- `load` - Loads the files generated in the `generate` operation into the database. You can use the `append` option to specify if the data needs to be appended to the existing directory data. For load to succeed, the LDAP server must be stopped. You can optionally specify the number of threads. If you set the `ldplonly` option to "TRUE", then the data is loaded in parallel but index creation takes place in serial mode. You must run a `generate` operation before a `load` operation.
- `recover` - In case of a failure during a load operation, recovers the directory with the original data. You cannot use any other option when using the `recover` option.
- `index` - Recreates indexes on all catalog tables.
- `missing` - Creates only missing indexes on catalog tables.

**file**

Required for the `check` and `generate` operations. The fully qualified path or relative path and file name of the LDIF file that contains the entries you want to load.

**threads**

Optional for the `check`, `generate`, and `load` operations. The number of threads to create. The default value is the number of CPUs on the machine plus one.

**restore**

Optional with the `check` and `generate` operations. Assumes operational attributes, such as `orclguid`, `creatorsname`, and `createtimestamp`, are already present in the specified LDIF file. Duplicate operational attribute values are not created in the output SQL\*Loader files.

When the `restore` option is set to `TRUE`, then the operational attributes specified in the LDIF file are honored. If `restore` option is not specified or it is set to `FALSE`, then the operational attributes might not be retained, depending on the type of attribute. Best practice is to avoid having operational attributes in the LDIF file when the `restore` option value is `FALSE`.

**append**

Optional with the `generate` and `load` operations. Loads entries in incremental mode rather than bulk mode, which is the default. Incremental mode appends data to existing directory data, and is intended for loading small amounts of data.

**encode**

Optional. The native character set encoding. Defaults to the character set of the user's terminal. Each supported character set has a unique acronym, for example, `WE8MSWIN1252`, `JA16SJIS`, or `AL32UTF8`.

**debug**

Optional. The `debug` option turns debugging on or off. Turning debugging on (`debug="TRUE"`) is useful when the command runs into errors. The output is logged to the `bulkload.log` file. This file can be found under `ORACLE_INSTANCE/diagnostics/logs/OID/tools`.

**verbose**

This is used to run the command in verbose mode.

### 3.2.3 Tasks and Examples for bulkload

Using the `bulkload` tool, you can perform the following tasks:

- [Section 3.2.3.1, "Loading Data in Bulk Mode"](#)
- [Section 3.2.3.2, "Loading Data for Multiple Nodes in a Replicated Environment"](#)
- [Section 3.2.3.3, "Loading Data in Incremental Mode"](#)
- [Section 3.2.3.4, "Verifying Indexes"](#)
- [Section 3.2.3.5, "Recreating Indexes"](#)
- [Section 3.2.3.6, "Recovering Data After a Load Error"](#)

### 3.2.3.1 Loading Data in Bulk Mode

The typical usage scenario is to load directory data after Oracle Internet Directory installation. First check the LDIF file for schema errors and generate the intermediate files. Next, load the data into the Oracle Internet Directory store.

The following example shows how to run the `bulkload` tool. The tool is first run with the `check` and `generate` options. The `check` option checks the input for schema and data consistency violations. The `generate` option generates the input files for SQL\*Loader. Next, the command is run with the `load` option to load the data into the directory.

**Example:**

```
bulkload connect="orcl" check="TRUE" generate="TRUE" file="~/myfiles/data.ldif"
bulkload connect="orcl" load="TRUE"
```

### 3.2.3.2 Loading Data for Multiple Nodes in a Replicated Environment

When you load the same data into multiple nodes in a replicated network, ensure that the `orclGUID` parameter (global ID) is consistent across all the nodes. You can accomplish this by generating the bulk load data file once only (using the `generate` argument), and then using the same data file to load the other nodes (using the `load` argument).

### 3.2.3.3 Loading Data in Incremental Mode

If you must add directory entries to an Oracle Internet Directory store already containing some user LDIF data, use the `append` argument to denote incremental mode. This mode is normally faster than other methods of adding entries to the directory. However, be sure that the directory server instances are in read-modify mode before you begin. The following example shows how to run `bulkload` in incremental mode.

**Example:**

```
bulkload connect="orcl" check="TRUE" generate="TRUE" load="TRUE" append="TRUE"
file="~/myfiles/data.ldif"
```

### 3.2.3.4 Verifying Indexes

You can verify existing indexes in the directory using the `check` option along with the `index` option.

**Example:**

```
bulkload connect="orcl" check="TRUE" index="TRUE"
```

### 3.2.3.5 Recreating Indexes

The `load` operation either updates or creates the indexes. However, due to issues like improper sizing, the indexes may not be updated or created properly. For this reason, the `bulkload` tool enables you to re-create all the indexes.

**Example:**

```
bulkload connect="orcl" index="TRUE"
```

### 3.2.3.6 Recovering Data After a Load Error

Due to issues like improper disk sizing, the load operation may fail. If this happens, then directory data can be inconsistent. For this reason, `bulkload` enables you to recover the directory data to the state that existed prior to the invocation of `bulkload`.

**Example:**

```
bulkload connect="orcl" recover="TRUE"
```

## 3.2.4 Related Command-Line Tools for `bulkload`

- See Section 3.1, "bulkdelete"
- See Section 3.3, "bulkmodify"
- See Section 3.5, "ldapadd"
- See Section 3.6, "ldapaddmt"

## 3.3 `bulkmodify`

The `bulkmodify` command-line tool enables you to modify a large number of existing entries in an efficient way.

---



---

**Note:** The `bulkmodify` command requires that the environment variable `ORACLE_INSTANCE` be set.

---



---

The `bulkmodify` tool supports the following:

- Subtree based modification
- LDAP search filter. For example, the filter could be `objectclass=*`, `objectclass=oneclass`, or `'(&(sn=Baileys)(cn=Kalid Baileys))'`.
- Attribute value addition and replacement. It modifies all matched entries in bulk.

The `bulkmodify` tool performs schema checking on the specified attribute name and value pair during initialization. All entries that meet the following criteria are modified:

- They are under the specified subtree.
- They meet the LDAP filter condition.
- They contain the attribute to be modified as either mandatory or optional.

The directory server and directory replication server may be running concurrently while bulk modification is in progress, but the bulk modification does not affect the replication server. You must perform bulk modification against all replicas.

---



---

**Note:**

LDIF file based modification is not supported by `bulkmodify`. This type of modification requires per-entry-based schema checking, and therefore the performance gain over the existing `ldapmodify` tool is insignificant.

Make sure that when `bulkmodify` is invoked, server side entry cache is disabled.

---



---

You must restrict user access to the subtree during bulk modification. If necessary, access control item (ACI) restriction can be applied to the subtree being updated by `bulkmodify`.

You cannot use `bulkmodify` to add a value to single-valued attributes that already contain one value. If a second value is added, you must alter the directory schema to make that attribute multi-valued.

The `bulkmodify` tool does not allow `add` or `replace` operations on the following attributes:

- `dn` (use `ldapmoddn` instead)
- `cn` (use `ldapmodify` instead)
- `userpassword` (use `ldapmodify` instead)
- `orclpassword` (use `ldapmodify` instead)
- `orclentrylevelaci` (use `ldapmodify` instead)
- `orclaci` (use `ldapmodify` instead)
- `orclcertificatehash`
- `orclcertificatematch`
- any binary attribute
- any operational attribute

It does not allow `replace` operation on the attribute `objectclass`.

It does not allow `add` for single-valued attributes.

### 3.3.1 Syntax for `bulkmodify`

```
bulkmodify connect=connect_string basedn=Base_DN
{[add="TRUE"|"FALSE"]|[replace="TRUE"|"FALSE"]} attribute=attribute_name
value=attribute_value [filter=filter_string] [size=transaction_size]
[threads=num_of_threads] [debug="TRUE"|"FALSE"] [encode=character_set]
[verbose="TRUE"|"FALSE"]
```

### 3.3.2 Arguments for `bulkmodify`

#### **connect**

Required. The directory database connect string. If you already have a `tnsnames.ora` file configured, then this is the net service name specified in that file, which is located by default in `ORACLE_INSTANCE/config`. (You can set the `TNS_ADMIN` environment variable if you want to use a different location.)

#### **basedn**

Required. The DN of the subtree to be modified. Enclose the DN in quotes.

#### **add | replace**

Required. The operation to be performed on the attribute. Specifies whether you want to add an attribute value or replace an attribute value.

#### **attribute**

Required. The name of a single attribute for which a value needs to be added or replaced.



**value**

Required. The single attribute value to add or replace. If the value contains spaces, enclose it in quotes.

**filter**

Optional. A filter string that contains a single attribute. Defaults to `objectclass=*`.

**size**

Optional. The number of entries to be committed as part of one transaction. Defaults to 100.

**threads**

Optional. The number of threads to create. The default value is the number of CPUs on the machine plus one.

**debug**

Optional. The debug option reports the logging level. This is useful in case the command runs into errors. The output is logged to the `bulkmodify.log` file. This file can be found under `ORACLE_INSTANCE/diagnostics/logs/OID/tools`.

**encode**

Optional. The native character set encoding. Defaults to the character set of the user's terminal. Each supported character set has a unique acronym, for example, `WE8MSWIN1252`, `JA16SJIS`, or `AL32UTF8`.

**verbose**

This is used to run the command in verbose mode.

### 3.3.3 Tasks and Examples for bulkmodify

Using the `bulkmodify` tool, you can perform the following task:

- [Section 3.3.3.1, "Updating an Attribute for Multiple Entries at Once"](#)

#### 3.3.3.1 Updating an Attribute for Multiple Entries at Once

The following example shows how to modify an attribute for several entries using a filter. This command adds the telephone number 408-123-4567 to the entries of all employees who have Anne Smith as their manager.

**Example:**

```
bulkmodify connect="orcl" basedn="c=US" add="TRUE" attribute="telephoneNumber"
value="408-123-4567" filter="manager=Anne Smith"
```

### 3.3.4 Limitations of bulkmodify

`bulkmodify` has the following limitations:

- `bulkmodify` does not distinguish between attributes with or without subtypes, when performing the `replace` operation. `bulkmodify` replaces the attribute value irrespective of whether the attribute contains subtypes.
- `bulkmodify` allows the RDN to be modified without modifying the DN. If an attribute is part of a DN, then the attribute value is modified but the DN entry in the directory is not modified.

- `bulkmodify` does not perform an object class check when performing an add operation. When adding a new attribute to a directory entry, `bulkmodify` does not verify if the entry has the required object class to support the attribute.

### 3.3.5 Related Command-Line Tools for `bulkmodify`

- See Section 3.1, "bulkdelete"
- See Section 3.2, "bulkload"
- See Section 3.11, "ldapmodify"
- See Section 3.12, "ldapmodifymt"

## 3.4 catalog

Oracle Internet Directory uses indexes to make attributes available for searches. When Oracle Internet Directory is installed, the `cn=catalogs` entry lists available attributes that can be used in a search. You can index only those attributes that have:

- An equality matching rule
- Matching rules supported by Oracle Internet Directory (see "Matching Rules" on page 6-4)

As of Oracle Internet Directory 11g Release 1 (11.1.1.6.0) a new autocatalog feature is enabled by default in fresh installs. You can also enable it if you have upgraded from a previous release. When this feature is enabled, Oracle Internet Directory automatically invokes the `catalog` command to index attributes when you search for them. If the autocatalog feature is not enabled, and you want to use previously uncataloged attributes in search filters, you must add them to the catalog entry, as in previous releases.

If the autocatalog feature is not enabled, and you want to use additional attributes in search filters, then you must add them to the catalog entry. You can do this at the time you create the attribute by using Oracle Directory Services Manager. However, if the attribute already exists, then you can index it only by using `ldapmodify` or the Catalog Management Tool (`catalog`).

---

---

**Notes:**

- As of Oracle Internet Directory 11g Release 1 (11.1.1.6.0), you can use the LDAP tool `ldapmodify` to create and drop indexes from attributes. The `ldapmodify` tool actually invokes `catalog`, and you can still use `catalog` for this purpose.
  - The `catalog` command requires that the environment variable `ORACLE_INSTANCE` be set.
  - The `catalog` command cannot index more than 1000 attributes at a time. If more than 1000 attributes are present in the file, the tool throws an error. If you need to index more than 1000 attributes, use multiple files.
- 
- 

Before running `catalog`, be sure that the directory server is either stopped or in read-only mode.

---



---

**Caution:** Do not use the catalog `delete="TRUE"` argument on indexes created by the Oracle Internet Directory base schema. Removing indexes from base schema attributes can adversely impact the operation of Oracle Internet Directory.

---



---

### 3.4.1 Syntax for catalog

```
catalog connect=connect_string {[add="TRUE"|"FALSE"]|[delete="TRUE"|"FALSE"]}
{[attribute=attribute_name]|[file=file_name]} [logging="TRUE"|"FALSE"]
[threads=num_of_threads] [debug="TRUE"|"FALSE"] [iot="TRUE"|"FALSE"]
[verbose="TRUE"|"FALSE"]
```

### 3.4.2 Arguments for catalog

#### **connect**

Required. The directory database connect string. If you already have a `tnsnames.ora` file configured, then this is the net service name specified in that file, which is located by default in `ORACLE_INSTANCE/config`. (You can set the `TNS_ADMIN` environment variable if you want to use a different location.)

#### **add | delete**

Required. The operation to perform. The `add` argument indexes the specified attribute. The `delete` argument drops the index for the specified attribute.

#### **attribute | file**

Required. The attribute or attributes to catalog. Use the `attribute` argument to specify a single attribute name on the command-line. Use the `file` argument to provide the full path and file name of a file that contains a list of several attribute names.

#### **logging**

Optional. This option is used to decide if redo logs are generated when a catalog is created.

#### **threads**

Optional. The number of threads to create. The default value is the number of CPUs on the machine plus one.

#### **debug**

Optional. The `debug` option reports the logging level. This is useful in case the command runs into errors. The output is logged to the `catalog.log` file. This file can be found under `ORACLE_INSTANCE/diagnostics/logs/OID/tools`.

#### **iot**

Optional. If set to `TRUE`, this option causes an Index Organized Table (IOT) to be created for the specified attribute without creating an additional index. The IOT option improves both read and write performance for a normal LDAP operation and reduces the storage as well. Use the IOT option when you expect lot of updates for the cataloging attribute. The default is `FALSE`.

#### **verbose**

Optional. This option specifies whether the command should be run in verbose mode.

### 3.4.3 Tasks and Examples for catalog

Using the catalog tool, you can perform the following tasks:

- [Section 3.4.3.1, "Indexing a Single Attribute"](#)
- [Section 3.4.3.2, "Indexing Multiple Attributes"](#)
- [Section 3.4.3.3, "Removing an Attribute from the List of Indexed Attributes"](#)
- [Section 3.4.3.4, "Indexing an Attribute Using the IOT Option"](#)

#### 3.4.3.1 Indexing a Single Attribute

The following example shows how to index a single attribute. The catalog tool prompts you for the Oracle Internet Directory superuser password.

**Example:**

```
catalog connect="orcl" add="TRUE" attribute="orclGender"
```

#### 3.4.3.2 Indexing Multiple Attributes

The following example shows how to index multiple values at once by supplying a file that contains a list of attribute names. The catalog tool prompts you for the Oracle Internet Directory superuser password.

**Example:**

```
catalog connect="orcl" add="TRUE" file="~/myfiles/attrs.txt"
```

#### 3.4.3.3 Removing an Attribute from the List of Indexed Attributes

The following example shows how to remove a single attribute from the list of indexed attributes. The catalog tool prompts you for the Oracle Internet Directory superuser password.

**Example:**

```
catalog connect="orcl" delete="TRUE" attribute="orclGender"
```

#### 3.4.3.4 Indexing an Attribute Using the IOT Option

The following example indexes the specified attribute and creates an IOT table to improve performance by not creating an additional index. The catalog tool prompts you for the Oracle Internet Directory superuser password.

**Example:**

```
catalog connect="orcl" attribute="orclGender" add="TRUE" iot="TRUE"
```

### 3.4.4 Related Command-Line Tools for catalog

- N/A

## 3.5 ldapadd

The ldapadd command-line tool enables you to add entries, their object classes, attributes, and values to the directory. To add attributes to an existing entry, use the ldapmodify command, explained in [Section 3.11, "ldapmodify"](#) on page 3-32.

**See Also:** For information on using attribute aliases with ldapadd refer to the "Attribute Aliases In the Directory" section in *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*

### 3.5.1 Syntax for ldapadd

```
ldapadd -h oid_hostname -D "binddn" -q | -w password [-Y "proxy_dn"]
[-p ldap_port] [-V ldap_version] {-f ldif_filename | -X dsml_filename}
[-b] [-n] [-c [-o log_file_name]] [-M] [-v] [-O ref_hop_limit] [-i 1|0]
[-U SSL_auth_mode {-W wallet_location -Q | -P wallet_password}]
[-d debug_level] [-E character_set]
```

### 3.5.2 Arguments for ldapadd

#### **-h oid\_hostname**

Required. The host name or IP address of the Oracle Internet Directory server.

#### **-D "binddn"**

Required. The DN of the Oracle Internet Directory user needed to bind to the directory (for example, cn=orcladmin).

#### **-q**

Required unless `-w` is used. Causes the command to prompt for the user password needed to bind to the directory. A password supplied at the command prompt is not visible on the screen.

#### **-w password**

Required unless `-q` is used. The user password needed to bind to the directory. Avoid supplying a password on the command line whenever possible. A password typed on the command line is visible on your screen. The `-w password` option is disabled when `LDAP_PASSWORD_PROMPTONLY` is set to true. See [Section 1.1, "Using Passwords with Command-Line Tools."](#)

#### **-Y "proxy\_dn"**

Optional. The DN of a proxy user. After binding to the directory, the add operation is performed as this user.

#### **-p ldap\_port**

Optional. The port number used to connect to the Oracle Internet Directory server. Defaults to port 3060.

#### **-V ldap\_version**

Optional. The version of the LDAP protocol to use. Allowed values are 2 or 3. Defaults to 3 (LDAP v3).

#### **-f ldif\_filename | -X dsml\_filename**

Required. The full path and file name of the input file that contains the data you want to import.

Use the `-f` argument to supply an LDIF file. See [Appendix A, "LDIF File Format"](#) for information on formatting an LDIF file.

Use the `-x` argument to supply a Directory Service Markup Language (DSML) file. See [Section 3.5.3.2, "Adding Data to the Directory Using a DSML File"](#) for more information about formatting a DSML file.

**-b**

Optional. Use this option if your input file has binary file names in it, which are preceded by the forward slash character. The tool retrieves the actual values from the file referenced.

**-n**

Optional. Enables you to preview what would occur in an operation without actually performing the operation.

**-c**

Optional. Proceeds in spite of errors. All errors are reported. If the `-c` argument is not used, the tool stops when an error occurs.

**-o log\_file\_name**

Optional. Used with the `-c` argument. Writes the LDIF entries with errors to a log file. Specify the full path and name of the log file.

**-M**

Optional. Instructs the tool to send the `ManageDSAIT` control to the server. The `ManageDSAIT` control instructs the server not to send referrals to clients. Instead a referral entry is returned as a regular entry.

**-v**

Optional. Runs the tool in verbose mode.

**-O ref\_hop\_limit**

Optional. The number of referral hops that a client should process. Defaults to 5.

**-i 1 | 0**

Optional. Specifies whether to bind as the current user when following referrals. 1 means bind as the current user, 0 means bind anonymously. The default is 0 (zero).

**-U SSL\_auth\_mode**

Optional. The SSL authentication mode:

- 1 for no authentication required.
- 2 for one way authentication required. You must also supply a wallet location and wallet password.
- 3 for two way authentication required. You must also supply a wallet location and wallet password.

**-W wallet\_location**

Required if using one way or two way SSL authentication (`-U 2|3`). The location of the wallet file that contains the server's SSL certificates.

Example for UNIX:

```
-W "file:/home/my_dir/my_wallet"
```

Example for Microsoft Windows:

```
-W "file:C:\my_dir\my_wallet"
```

#### **-Q**

Required, unless `-P` is used, if using one way or two way SSL authentication (`-U 2|3`). Causes the command to prompt for the wallet password for the wallet specified in the `-W` argument. A password supplied at the command prompt is not visible on the screen.

#### **-P wallet\_password**

Required, unless `-Q` is used, if using one way or two way SSL authentication (`-U 2|3`). The wallet password for the wallet specified in the `-W` argument. Avoid supplying a password on the command line whenever possible. A password typed on the command line is visible on your screen. The `-P wallet_password` option is disabled when `LDAP_PASSWORD_PROMPTONLY` is set to true. See [Section 1.1, "Using Passwords with Command-Line Tools."](#)

#### **-d debug\_level**

Optional. If not specified the default of 0 (not enabled) is used. Debug levels are additive. Add the numbers representing the functions that you want to activate, and use the sum of those in the command-line option. For example, to trace search filter processing (512) and active connection management (256), enter 768 as the debug level (512 + 256 = 768). Debug levels are as follows:

- 1 — Heavy trace debugging
- 128 — Debug packet handling
- 256 — Connection management, related to network activities
- 512 — Search filter processing
- 1024 — Entry parsing
- 2048 — Configuration file processing
- 8192 — Access control list processing
- 491520 — Log of communication with the database
- 524288 — Schema related operations
- 4194304 — Replication specific operations
- 8388608 — Log of entries, operations and results for each connection
- 16777216 — Trace function call arguments
- 67108864 — Number and identity of clients connected to this server
- 117440511 — All possible operations and data

#### **-E character\_set**

Optional. The native character set encoding. Defaults to the character set of the user's terminal. Each supported character set has a unique acronym, for example, `WE8MSWIN1252`, `JA16SJIS`, or `AL32UTF8`.

### 3.5.3 Tasks and Examples for ldapadd

Using the ldapadd tool, you can perform the following tasks:

- Section 3.5.3.1, "Adding Data to the Directory Using an LDIF File"
- Section 3.5.3.2, "Adding Data to the Directory Using a DSML File"
- Section 3.5.3.3, "Previewing an Add Operation"

### 3.5.3.1 Adding Data to the Directory Using an LDIF File

You can use `ldapadd` to add entries or schema information to the directory from an LDIF file. The file must be correctly formatted. See [Appendix A, "LDIF File Format"](#) for information about formatting an LDIF file.

#### Example:

```
ldapadd -h myhost.company.com -D "cn=orcladmin" -q -p 3060 \  
-f ~/myfiles/input.ldif -v
```

### 3.5.3.2 Adding Data to the Directory Using a DSML File

You can use `ldapadd` to add entries or schema information to the directory from a Directory Service Markup Language (DSML) file that contains `<addRequest>` elements. For more information about the formatting DSML files, visit the OASIS Web site at <http://www.oasis-open.org>. The following example shows a sample DSML entry for a user.

#### Example:

```
<addRequest dn="CN=Alice,OU=HR,DC=Example,DC=COM">  
  <attr name="objectclass"><value>top</value></attr>  
  <attr name="objectclass"><value>person</value></attr>  
  <attr name="objectclass"><value>organizationalPerson</value></attr>  
  <attr name="sn"><value>Johnson</value></attr>  
  <attr name="givenName"><value>Alice</value></attr>  
  <attr name="title"><value>Software Design Engineer</value></attr>  
</addRequest>
```

Once you have a correctly formatted DSML file, you can add data to the directory using `ldapadd` and supplying the DSML file as the input file.

#### Example:

```
ldapadd -h myhost.company.com -D "cn=orcladmin" -q -p 3060 \  
-X ~/myfiles/input.xml -v
```

### 3.5.3.3 Previewing an Add Operation

Use the `-n` argument with an `ldapadd` command to preview the results of an add operation before actually adding any data to the directory.

#### Example:

```
ldapadd -h myhost.company.com -D "cn=orcladmin" -q -p 3060 \  
-X ~/myfiles/input.xml -v -n
```

## 3.5.4 Related Command-Line Tools for ldapadd

- See [Section 3.6, "ldapaddmt"](#)
- See [Section 3.11, "ldapmodify"](#)
- See [Section 3.2, "bulkload"](#)



## 3.6 ldapaddmt

The `ldapaddmt` tool performs the same functionality as the `ldapadd` command. It enables you to add entries, their object classes, attributes, and values to the directory. However, it also supports multiple threads for adding entries concurrently.

While it is processing entries, `ldapaddmt` logs errors in the `add.log` file within the current directory.

**Note:** Increasing the number of concurrent threads improves the rate at which entries are created, but consumes more system resources.

### 3.6.1 Syntax for ldapaddmt

```
ldapaddmt -h oid_hostname -D "binddn" -q | -w password -T number_threads
[-p ldap_port] [-V ldap_version] {-f ldif_filename | -X dsml_filename} [-b] [-c]
[-M] [-O ref_hop_limit] [-U SSL_auth_mode {-W wallet_location -Q | -P
wallet_password}] [-d debug_level] [-E character_set]
```

### 3.6.2 Arguments for ldapaddmt

#### **-h oid\_hostname**

Required. The host name or IP address of the Oracle Internet Directory server.

#### **-D "binddn"**

Required. The DN of the Oracle Internet Directory user needed to bind to the directory (for example, `cn=orcladmin`).

#### **-q**

Required unless `-w` is used. Causes the command to prompt for the user password needed to bind to the directory. A password supplied at the command prompt is not visible on the screen.

#### **-w password**

Required unless `-q` is used. The user password needed to bind to the directory. Avoid supplying a password on the command line whenever possible. A password typed on the command line is visible on your screen. The `-w password` option is disabled when `LDAP_PASSWORD_PROMPTONLY` is set to true. See [Section 1.1, "Using Passwords with Command-Line Tools."](#)

#### **-T number\_threads**

Required. The number of threads for concurrently processing entries.

#### **-p ldap\_port**

Optional. The port number used to connect to the Oracle Internet Directory server. Defaults to port 3060.

#### **-V ldap\_version**

Optional. The version of the LDAP protocol to use. Allowed values are 2 or 3. Defaults to 3 (LDAP v3).

**-f ldif\_filename | -X dsml\_filename**

Required. The full path and file name of the input file that contains the data you want to import.

Use the `-f` argument to supply an LDIF file. See [Appendix A, "LDIF File Format"](#) for information on formatting an LDIF file.

Use the `-X` argument to supply a Directory Service Markup Language (DSML) file. See [Section 3.5.3.2, "Adding Data to the Directory Using a DSML File"](#) for more information about formatting a DSML file.

**-b**

Optional. Use this option if your input file has binary file names in it, which are preceded by the forward slash character. The tool retrieves the actual values from the file referenced.

**-c**

Optional. Proceeds in spite of errors. All errors are reported. If the `-c` argument is not used, the tool stops when an error occurs.

**-M**

Optional. Instructs the tool to send the `ManageDSAIT` control to the server. The `ManageDSAIT` control instructs the server not to send referrals to clients. Instead a referral entry is returned as a regular entry.

**-O ref\_hop\_limit**

Optional. The number of referral hops that a client should process. Defaults to 5.

**-U SSL\_auth\_mode**

Optional. The SSL authentication mode:

- 1 for no authentication required.
- 2 for one way authentication required. You must also supply a wallet location and wallet password.
- 3 for two way authentication required. You must also supply a wallet location and wallet password.

**-W wallet\_location**

Required if using one way or two way SSL authentication (`-U 2|3`). The location of the wallet file that contains the server's SSL certificates.

Example for UNIX:

```
-W "file:/home/my_dir/my_wallet"
```

Example for Microsoft Windows:

```
-W "file:C:\my_dir\my_wallet"
```

**-Q**

Required, unless `-P` is used, if using one way or two way SSL authentication (`-U 2|3`). Causes the command to prompt for the wallet password for the wallet specified in the `-W` argument. A password supplied at the command prompt is not visible on the screen.

**-P wallet\_password**

Required, unless `-Q` is used, if using one way or two way SSL authentication (`-U 2|3`). The wallet password for the wallet specified in the `-W` argument. Avoid supplying a password on the command line whenever possible. A password typed on the command line is visible on your screen. The `-P wallet_password` option is disabled when `LDAP_PASSWORD_PROMPTONLY` is set to true. See [Section 1.1, "Using Passwords with Command-Line Tools."](#)

**-d debug\_level**

Optional. If not specified the default of 0 (not enabled) is used. Debug levels are additive. Add the numbers representing the functions that you want to activate, and use the sum of those in the command-line option. For example, to trace search filter processing (512) and active connection management (256), enter 768 as the debug level (512 + 256 = 768). Debug levels are as follows:

- 1 — Heavy trace debugging
- 128 — Debug packet handling
- 256 — Connection management, related to network activities
- 512 — Search filter processing
- 1024 — Entry parsing
- 2048 — Configuration file processing
- 8192 — Access control list processing
- 491520 — Log of communication with the database
- 524288 — Schema related operations
- 4194304 — Replication specific operations
- 8388608 — Log of entries, operations and results for each connection
- 16777216 — Trace function call arguments
- 67108864 — Number and identity of clients connected to this server
- 117440511 — All possible operations and data

**-E character\_set**

Optional. The native character set encoding. Defaults to the character set of the user's terminal. Each supported character set has a unique acronym, for example, `WE8MSWIN1252`, `JA16SJIS`, or `AL32UTF8`.

### 3.6.3 Tasks and Examples for ldapaddmt

Using the `ldapaddmt` tool, you can perform the following task:

- [Section 3.6.3.1, "Adding Concurrent Entries to the Directory Using an LDIF File"](#)

#### 3.6.3.1 Adding Concurrent Entries to the Directory Using an LDIF File

You can use `ldapaddmt` to add concurrent entries or schema information to the directory from an LDIF file. The file must be correctly formatted. See [Appendix A, "LDIF File Format"](#) for information about formatting an LDIF file.

**Example:**

```
ldapaddmt -h myhost.company.com -D "cn=orcladmin" -q -T 5 -p 3060 \
```

```
-f ~/myfiles/input.ldif -v
```

### 3.6.4 Related Command-Line Tools for ldapaddmt

- See Section 3.5, "ldapadd"
- See Section 3.2, "bulkload"

## 3.7 ldapbind

The `ldapbind` command-line tool enables you to see whether you can authenticate a client to a server.

### 3.7.1 Syntax for ldapbind

```
ldapbind -h oid_hostname -D "binddn" -q | -w password [-p ldap_port]
[-V ldap_version] [-n] [-O "auth"] [-Y "DIGEST-MD5|EXTERNAL"]
[-R SASL_realm] [-U SSL_auth_mode {-W wallet_location -Q | -P wallet_password}]
[-E character_set]
```

### 3.7.2 Arguments for ldapbind

**-h oid\_hostname**

Required. The host name or IP address of the Oracle Internet Directory server.

**-D "binddn"**

Required. The DN of the Oracle Internet Directory user needed to bind to the directory (for example, `cn=orcladmin`).

**-q**

Required unless `-w` is used. Causes the command to prompt for the user password needed to bind to the directory. A password supplied at the command prompt is not visible on the screen.

**-w password**

Required unless `-q` is used. The user password needed to bind to the directory. Avoid supplying a password on the command line whenever possible. A password typed on the command line is visible on your screen. The `-w password` option is disabled when `LDAP_PASSWORD_PROMPTONLY` is set to `true`. See Section 1.1, "Using Passwords with Command-Line Tools."

**-p ldap\_port**

Optional. The port number used to connect to the Oracle Internet Directory server. Defaults to port 3060.

**-V ldap\_version**

Optional. The version of the LDAP protocol to use. Allowed values are 2 or 3. Defaults to 3 (LDAP v3).

**-O "auth"**

Optional. Specifies SASL security properties. The security property supported is `-O "auth"`. This security property is for `DIGEST-MD5` SASL mechanism. It enables authentication with no data integrity or data privacy.

**-Y "DIGEST-MD5 | EXTERNAL"**

Optional. Specifies a Simple Authentication and Security Layer (SASL) mechanism. The following mechanisms are supported:

- DIGEST-MD5
- EXTERNAL - The SASL authentication in this mechanism is done on top of two-way SSL authentication. In this case the identity of the user stored in the SSL wallet is used for SASL authentication.

**-R SASL\_realm**

Optional. A SASL realm.

**-U SSL\_auth\_mode**

Optional. The SSL authentication mode:

- 1 for no authentication required.
- 2 for one way authentication required. You must also supply a wallet location and wallet password.
- 3 for two way authentication required. You must also supply a wallet location and wallet password.

**-W wallet\_location**

Required if using one way or two way SSL authentication (-U 2|3). The location of the wallet file that contains the server's SSL certificates.

Example for UNIX:

```
-W "file:/home/my_dir/my_wallet"
```

Example for Microsoft Windows:

```
-W "file:C:\my_dir\my_wallet"
```

**-Q**

Required, unless -P is used, if using one way or two way SSL authentication (-U 2|3). Causes the command to prompt for the wallet password for the wallet specified in the -W argument. A password supplied at the command prompt is not visible on the screen.

**-P wallet\_password**

Required, unless -Q is used, if using one way or two way SSL authentication (-U 2|3). The wallet password for the wallet specified in the -W argument. Avoid supplying a password on the command line whenever possible. A password typed on the command line is visible on your screen. The -P *wallet\_password* option is disabled when LDAP\_PASSWORD\_PROMPTONLY is set to true. See [Section 1.1, "Using Passwords with Command-Line Tools."](#)

**-E character\_set**

Optional. The native character set encoding. Defaults to the character set of the user's terminal. Each supported character set has a unique acronym, for example, WE8MSWIN1252, JA16SJIS, or AL32UTF8.

### 3.7.3 Tasks and Examples for ldapbind

Using the ldapbind tool, you can perform the following task:

- [Section 3.7.3.1, "Validating Authentication Credentials"](#)

### 3.7.3.1 Validating Authentication Credentials

The following example shows how to validate the authentication credentials used to bind to the directory server when using SSL.

**Example:**

```
ldapbind -h myhost.company.com -D "cn-orcladmin" -q -p 3133 \  
-U 2 -W "file:/home/my_dir/my_wallet" -Q
```

## 3.7.4 Related Command-Line Tools for ldapbind

- N/A

## 3.8 ldapcompare

The ldapcompare command-line tool enables you to compare an attribute value that you specify on the command line to the attribute value in a directory entry.

### 3.8.1 Syntax for ldapcompare

```
ldapcompare -h oid_hostname -D "binddn" -q | -w password [-Y "proxy_dn"]  
[-p ldap_port] -a attribute_name -b "base" -v "attribute_value"  
[-U SSL_auth_mode {-W wallet_location -Q | -P wallet_password}]  
[-d debug_level] [-E character_set]
```

### 3.8.2 Arguments for ldapcompare

**-h oid\_hostname**

Required. The host name or IP address of the Oracle Internet Directory server.

**-D "binddn"**

Required. The DN of the Oracle Internet Directory user needed to bind to the directory (for example, cn=orcladmin).

**-q**

Required unless `-w` is used. Causes the command to prompt for the user password needed to bind to the directory. A password supplied at the command prompt is not visible on the screen.

**-w password**

Required unless `-q` is used. The user password needed to bind to the directory. Avoid supplying a password on the command line whenever possible. A password typed on the command line is visible on your screen. The `-w password` option is disabled when `LDAP_PASSWORD_PROMPTONLY` is set to true. See [Section 1.1, "Using Passwords with Command-Line Tools."](#)

**-Y "proxy\_dn"**

Optional. The DN of a proxy user. After binding to the directory, the add operation is performed as this user.

**-p ldap\_port**

Optional. The port number used to connect to the Oracle Internet Directory server. Defaults to port 3060.

**-a attribute\_name**

Required. The attribute for which to perform the comparison of values.

**-b "base"**

Required. The DN of the entry for which to perform the comparison.

**-v "attribute\_value"**

Required. The attribute value that you want to compare to the value in the entry.

**-U SSL\_auth\_mode**

Optional. The SSL authentication mode:

- 1 for no authentication required.
- 2 for one way authentication required. You must also supply a wallet location and wallet password.
- 3 for two way authentication required. You must also supply a wallet location and wallet password.

**-W wallet\_location**

Required if using one way or two way SSL authentication (-U 2|3). The location of the wallet file that contains the server's SSL certificates.

Example for UNIX:

```
-W "file:/home/my_dir/my_wallet"
```

Example for Microsoft Windows:

```
-W "file:C:\my_dir\my_wallet"
```

**-Q**

Required, unless -P is used, if using one way or two way SSL authentication (-U 2|3). Causes the command to prompt for the wallet password for the wallet specified in the -W argument. A password supplied at the command prompt is not visible on the screen.

**-P wallet\_password**

Required, unless -Q is used, if using one way or two way SSL authentication (-U 2|3). The wallet password for the wallet specified in the -W argument. Avoid supplying a password on the command line whenever possible. A password typed on the command line is visible on your screen. The -P *wallet\_password* option is disabled when LDAP\_PASSWORD\_PROMPTONLY is set to true. See [Section 1.1, "Using Passwords with Command-Line Tools."](#)

**-d debug\_level**

Optional. If not specified the default of 0 (not enabled) is used. Debug levels are additive. Add the numbers representing the functions that you want to activate, and use the sum of those in the command-line option. For example, to trace search filter processing (512) and active connection management (256), enter 768 as the debug level (512 + 256 = 768). Debug levels are as follows:

- 1 — Heavy trace debugging
- 128 — Debug packet handling
- 256 — Connection management, related to network activities
- 512 — Search filter processing
- 1024 — Entry parsing
- 2048 — Configuration file processing
- 8192 — Access control list processing
- 491520 — Log of communication with the database
- 524288 — Schema related operations
- 4194304 — Replication specific operations
- 8388608 — Log of entries, operations and results for each connection
- 16777216 — Trace function call arguments
- 67108864 — Number and identity of clients connected to this server
- 117440511 — All possible operations and data

**-E character\_set**

Optional. The native character set encoding. Defaults to the character set of the user's terminal. Each supported character set has a unique acronym, for example, WE8MSWIN1252, JA16SJIS, or AL32UTF8.

### 3.8.3 Tasks and Examples for ldapcompare

Using `ldapcompare` you can perform the following task:

- [Section 3.8.3.1, "Comparing Attribute Values for an Entry"](#)

#### 3.8.3.1 Comparing Attribute Values for an Entry

The following example shows how to check an entry for a person named *Anne Smith* to see if her *title* is *Manager*.

**Example:**

```
ldapcompare -h myhost.company.com -D "cn=orcladmin" -q -p 3060 -a title \  
-b "cn=Anne Smith,ou=Sales,o=IMC,c=US" -v "Manager"
```

### 3.8.4 Related Command-Line Tools for ldapcompare

- N/A

## 3.9 ldapdelete

The `ldapdelete` command-line tool enables you to remove entire entries from the directory.

**See Also:** For information on using attribute aliases with `ldapdelete` refer to the "Attribute Aliases In the Directory" section in *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*



### 3.9.1 Syntax for ldapdelete

```
ldapdelete -h oid_hostname -D "binddn" -q | -w password [-Y proxy_dn]
[-p ldap_port] [-V ldap_version] {-f ldif_filename | "entry_dn"}
[-n] [-M] [-v] [-O ref_hop_limit]
[-U SSL_auth_mode {-W wallet_location -Q | -P wallet_password}] [-E character_set]
```

### 3.9.2 Arguments for ldapdelete

#### **-h oid\_hostname**

Required. The host name or IP address of the Oracle Internet Directory server.

#### **-D "binddn"**

Required. The DN of the Oracle Internet Directory user needed to bind to the directory (for example, cn=orcladmin).

#### **-q**

Required unless `-w` is used. Causes the command to prompt for the user password needed to bind to the directory. A password supplied at the command prompt is not visible on the screen.

#### **-w password**

Required unless `-q` is used. The user password needed to bind to the directory. Avoid supplying a password on the command line whenever possible. A password typed on the command line is visible on your screen. The `-w password` option is disabled when `LDAP_PASSWORD_PROMPTONLY` is set to `true`. See [Section 1.1, "Using Passwords with Command-Line Tools."](#)

#### **-Y "proxy\_dn"**

Optional. The DN of a proxy user. After binding to the directory, the add operation is performed as this user.

#### **-p ldap\_port**

Optional. The port number used to connect to the Oracle Internet Directory server. Defaults to port 3060.

#### **-V ldap\_version**

Optional. The version of the LDAP protocol to use. Allowed values are 2 or 3. Defaults to 3 (LDAP v3).

#### **-f ldif\_filename | "entry\_dn"**

Required. The full path and file name of the input file that contains the entry DNs you want to delete, or a single entry DN supplied on the command-line.

Use the `-f` argument to supply an LDIF file. See [Appendix A, "LDIF File Format"](#) for information on formatting an LDIF file.

To delete one entry, supply the DN of the entry in quotes.

#### **-n**

Optional. Enables you to preview what would occur in an operation without actually performing the operation.

**-M**

Optional. Instructs the tool to send the `ManageDSAIT` control to the server. The `ManageDSAIT` control instructs the server not to send referrals to clients. Instead a referral entry is returned as a regular entry.

**-v**

Optional. Runs the tool in verbose mode.

**-O ref\_hop\_limit**

Optional. The number of referral hops that a client should process. Defaults to 5.

**-U SSL\_auth\_mode**

Optional. The SSL authentication mode:

- 1 for no authentication required.
- 2 for one way authentication required. You must also supply a wallet location and wallet password.
- 3 for two way authentication required. You must also supply a wallet location and wallet password.

**-W wallet\_location**

Required if using one way or two way SSL authentication (`-U 2|3`). The location of the wallet file that contains the server's SSL certificates.

Example for UNIX:

```
-W "file:/home/my_dir/my_wallet"
```

Example for Microsoft Windows:

```
-W "file:C:\my_dir\my_wallet"
```

**-Q**

Required, unless `-P` is used, if using one way or two way SSL authentication (`-U 2|3`). Causes the command to prompt for the wallet password for the wallet specified in the `-W` argument. A password supplied at the command prompt is not visible on the screen.

**-P wallet\_password**

Required, unless `-Q` is used, if using one way or two way SSL authentication (`-U 2|3`). The wallet password for the wallet specified in the `-W` argument. Avoid supplying a password on the command line whenever possible. A password typed on the command line is visible on your screen. The `-P wallet_password` option is disabled when `LDAP_PASSWORD_PROMPTONLY` is set to true. See [Section 1.1, "Using Passwords with Command-Line Tools."](#)

**-E character\_set**

Optional. The native character set encoding. Defaults to the character set of the user's terminal. Each supported character set has a unique acronym, for example, `WE8MSWIN1252`, `JA16SJIS`, or `AL32UTF8`.

### 3.9.3 Tasks and Examples for ldapdelete

Using `ldapdelete` you can perform the following tasks:

- Section 3.9.3.1, "Deleting a Single Entry"
- Section 3.9.3.2, "Deleting Multiple Entries Using an LDIF File"

### 3.9.3.1 Deleting a Single Entry

The following example shows how to delete an entry for a person named *Anne Smith*.

**Example:**

```
ldapdelete -h myhost.company.com -D "cn=orcladmin" -q \
-p 3060 "cn=Anne Smith,ou=Sales,o=IMC,c=US"
```

### 3.9.3.2 Deleting Multiple Entries Using an LDIF File

The following example shows how to delete many entries at once by supplying an LDIF file that contains the DNs of the entries to delete. See [Appendix A, "LDIF File Format"](#) for information about formatting an LDIF file.

**Example:**

```
ldapdelete -h myhost.company.com -D "cn=orcladmin" -q -p 3060 \
/home/mydir/delete.ldif -f
```

## 3.9.4 Related Command-Line Tools for ldapdelete

- See [Section 3.1, "bulkdelete"](#)

## 3.10 ldapmoddn

The `ldapmoddn` command-line tool enables you to change the RDN of an entry, or to move an entry to a new parent node in the directory tree.

**See Also:** For information on using attribute aliases with `ldapmoddn` refer to the "Attribute Aliases In the Directory" section in *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*

### 3.10.1 Syntax for ldapmoddn

```
ldapmoddn -h oid_hostname -D "binddn" -q | -w password [-p ldap_port]
[-V ldap_version] -b "base_dn" {-R "new_rdn"|-N "new_parent"}
[-r] [-M] [-O ref_hop_limit]
[-U SSL_auth_mode {-W wallet_location -Q | -P wallet_password}] [-E character_set]
```

### 3.10.2 Arguments for ldapmoddn

**-h oid\_hostname**

Required. The host name or IP address of the Oracle Internet Directory server.

**-D "binddn"**

Required. The DN of the Oracle Internet Directory user needed to bind to the directory (for example, `cn=orcladmin`).

**-q**

Required unless `-w` is used. Causes the command to prompt for the user password needed to bind to the directory. A password supplied at the command prompt is not visible on the screen.

**-w password**

Required unless `-q` is used. The user password needed to bind to the directory. Avoid supplying a password on the command line whenever possible. A password typed on the command line is visible on your screen. The `-w password` option is disabled when `LDAP_PASSWORD_PROMPTONLY` is set to true. See [Section 1.1, "Using Passwords with Command-Line Tools."](#)

**-p ldap\_port**

Optional. The port number used to connect to the Oracle Internet Directory server. Defaults to port 3060.

**-V ldap\_version**

Optional. The version of the LDAP protocol to use. Allowed values are 2 or 3. Defaults to 3 (LDAP v3).

**-b "base\_dn"**

Required. The DN of the entry to be moved to a new parent DN or have its RDN updated.

**-R "new\_rdn" | -N "new\_parent"**

Required. The action to perform. Use the `-R` argument to change the RDN of the entry. Use the `-N` argument to move the entry to a new parent node in the directory tree.

**-r**

Optional. Specifies that the old RDN is not retained as a value in the modified entry. If not included, the old RDN is retained as an attribute in the modified entry.

**-M**

Optional. Instructs the tool to send the `ManageDSAIT` control to the server. The `ManageDSAIT` control instructs the server not to send referrals to clients. Instead a referral entry is returned as a regular entry.

**-O ref\_hop\_limit**

Optional. The number of referral hops that a client should process. Defaults to 5.

**-U SSL\_auth\_mode**

Optional. The SSL authentication mode:

- 1 for no authentication required.
- 2 for one way authentication required. You must also supply a wallet location and wallet password.
- 3 for two way authentication required. You must also supply a wallet location and wallet password.

**-W wallet\_location**

Required if using one way or two way SSL authentication (-U 2|3). The location of the wallet file that contains the server's SSL certificates.

Example for UNIX:

```
-W "file:/home/my_dir/my_wallet"
```

Example for Microsoft Windows:

```
-W "file:C:\my_dir\my_wallet"
```

**-Q**

Required, unless -P is used, if using one way or two way SSL authentication (-U 2|3). Causes the command to prompt for the wallet password for the wallet specified in the -W argument. A password supplied at the command prompt is not visible on the screen.

**-P wallet\_password**

Required, unless -Q is used, if using one way or two way SSL authentication (-U 2|3). The wallet password for the wallet specified in the -W argument. Avoid supplying a password on the command line whenever possible. A password typed on the command line is visible on your screen. The -P *wallet\_password* option is disabled when LDAP\_PASSWORD\_PROMPTONLY is set to true. See [Section 1.1, "Using Passwords with Command-Line Tools."](#)

**-E character\_set**

Optional. The native character set encoding. Defaults to the character set of the user's terminal. Each supported character set has a unique acronym, for example, WE8MSWIN1252, JA16SJIS, or AL32UTF8.

### 3.10.3 Tasks and Examples for ldapmoddn

Using the ldapmoddn command-line tool, you can perform the following tasks:

- [Section 3.10.3.1, "Changing the RDN of an Entry"](#)
- [Section 3.10.3.2, "Moving an Entry"](#)

#### 3.10.3.1 Changing the RDN of an Entry

The following example shows how to change the RDN of an entry from *Mary Smith* to *Mary Jones*.

**Example:**

```
ldapmoddn -h myhost.company.com -D "cn=orcladmin" -q -p 3060 \
  -b "cn=Mary Smith,dc=Americas,dc=IMC,dc=com" -R "cn=Mary Jones" -r
```

#### 3.10.3.2 Moving an Entry

The following example shows how to move an entry to another parent node in the directory subtree. The entry with the RDN of *Mary Smith* is moved from the *dc=Americas* parent node to the *dc=Australia* parent node.

**Example:**

```
ldapmoddn -h myhost.company.com -D "cn=orcladmin" -q -p 3060 \
  -b "cn=Mary Smith,dc=Americas,dc=IMC,dc=com" -N "dc=Australia,dc=IMC,dc=com"
```

### 3.10.4 Related Command-Line Tools for ldapmoddn

- See [Section 3.11, "ldapmodify"](#)

## 3.11 ldapmodify

The `ldapmodify` command-line tool enables you to add, delete, or replace attributes for entries by supplying an LDIF file as input. You can also delete or add entries using `ldapmodify`.

See [Appendix A, "LDIF File Format"](#) for more information about the correct formatting of LDIF files.

**See Also:** For information on using attribute aliases with `ldapmodify` refer to the "Attribute Aliases In the Directory" section in *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*

### 3.11.1 Syntax for ldapmodify

```
ldapmodify -h oid_hostname -D "binddn" [-Y "proxy_dn"] -q | -w password
[-p ldap_port] [-V ldap_version] {-f ldif_filename | -X dsml_filename}
[-a] [-b] [-c [-o log_file_name]] [-n] [-v] [-M] [-O ref_hop_limit]
[-i 1|0] [-U SSL_auth_mode {-W wallet_location -Q | -P wallet_password}]
[-E character_set] [-d debug_level]
```

### 3.11.2 Arguments for ldapmodify

**-h oid\_hostname**

Required. The host name or IP address of the Oracle Internet Directory server.

**-D "binddn"**

Required. The DN of the Oracle Internet Directory user needed to bind to the directory (for example, `cn=orcladmin`).

**-Y "proxy\_dn"**

Optional. The DN of a proxy user. After binding to the directory, the add operation is performed as this user.

**-q**

Required unless `-w` is used. Causes the command to prompt for the user password needed to bind to the directory. A password supplied at the command prompt is not visible on the screen.

**-w password**

Required unless `-q` is used. The user password needed to bind to the directory. Avoid supplying a password on the command line whenever possible. A password typed on the command line is visible on your screen. The `-w password` option is disabled when `LDAP_PASSWORD_PROMPTONLY` is set to true. See [Section 1.1, "Using Passwords with Command-Line Tools."](#)

**-p ldap\_port**

Optional. The port number used to connect to the Oracle Internet Directory server. Defaults to port 3060.

**-V ldap\_version**

Optional. The version of the LDAP protocol to use. Allowed values are 2 or 3. Defaults to 3 (LDAP v3).

**-f ldif\_filename | -X dsml\_filename**

Required. The full path and file name of the input file that contains the data you want to import.

Use the `-f` argument to supply an LDIF file. See [Appendix A, "LDIF File Format"](#) for information on formatting an LDIF file.

Use the `-X` argument to supply a Directory Service Markup Language (DSML) file. See [Section 3.5.3.2, "Adding Data to the Directory Using a DSML File"](#) for more information about formatting a DSML file.

**-a**

Optional. Denotes that the LDIF or DSML input file has new entries to be added.

**-b**

Optional. Use this option if your input file has binary file names in it, which are preceded by the forward slash character. The tool retrieves the actual values from the file referenced.

**-c**

Optional. Proceeds in spite of errors. All errors are reported. If the `-c` argument is not used, the tool stops when an error occurs.

**-n**

Optional. Enables you to preview what would occur in an operation without actually performing the operation.

**-v**

Optional. Runs the tool in verbose mode.

**-o log\_file\_name**

Optional. Used with the `-c` argument. Writes the LDIF entries with errors to a log file. Specify the full path and name of the log file.

**-M**

Optional. Instructs the tool to send the `ManageDSAIT` control to the server. The `ManageDSAIT` control instructs the server not to send referrals to clients. Instead a referral entry is returned as a regular entry.

**-O ref\_hop\_limit**

Optional. The number of referral hops that a client should process. Defaults to 5.

**-i 1 | 0**

Optional. Specifies whether to bind as the current user when following referrals. 1 means bind as the current user, 0 means bind anonymously. The default is 0 (zero).

**-U SSL\_auth\_mode**

Optional. The SSL authentication mode:

- 1 for no authentication required.
- 2 for one way authentication required. You must also supply a wallet location and wallet password.
- 3 for two way authentication required. You must also supply a wallet location and wallet password.

**-W wallet\_location**

Required if using one way or two way SSL authentication (-U 2|3). The location of the wallet file that contains the server's SSL certificates.

Example for UNIX:

```
-W "file:/home/my_dir/my_wallet"
```

Example for Microsoft Windows:

```
-W "file:C:\my_dir\my_wallet"
```

**-Q**

Required, unless -P is used, if using one way or two way SSL authentication (-U 2|3). Causes the command to prompt for the wallet password for the wallet specified in the -W argument. A password supplied at the command prompt is not visible on the screen.

**-P wallet\_password**

Required, unless -Q is used, if using one way or two way SSL authentication (-U 2|3). The wallet password for the wallet specified in the -W argument. Avoid supplying a password on the command line whenever possible. A password typed on the command line is visible on your screen. The -P *wallet\_password* option is disabled when LDAP\_PASSWORD\_PROMPTONLY is set to true. See [Section 1.1, "Using Passwords with Command-Line Tools."](#)

**-E character\_set**

Optional. The native character set encoding. Defaults to the character set of the user's terminal. Each supported character set has a unique acronym, for example, WE8MSWIN1252, JA16SJIS, or AL32UTF8.

**-d debug\_level**

Optional. If not specified the default of 0 (not enabled) is used. Debug levels are additive. Add the numbers representing the functions that you want to activate, and use the sum of those in the command-line option. For example, to trace search filter processing (512) and active connection management (256), enter 768 as the debug level (512 + 256 = 768). Debug levels are as follows:

- 1 — Heavy trace debugging
- 128 — Debug packet handling
- 256 — Connection management, related to network activities
- 512 — Search filter processing
- 1024 — Entry parsing
- 2048 — Configuration file processing
- 8192 — Access control list processing
- 491520 — Log of communication with the database



- 524288 — Schema related operations
- 4194304 — Replication specific operations
- 8388608 — Log of entries, operations and results for each connection
- 16777216 — Trace function call arguments
- 67108864 — Number and identity of clients connected to this server
- 117440511 — All possible operations and data

### 3.11.3 Tasks and Examples for ldapmodify

Using the `ldapmodify` command-line tool, you can perform the following tasks:

- [Section 3.11.3.1, "Modifying the Directory Schema"](#)
- [Section 3.11.3.2, "Modifying an Entry"](#)
- [Section 3.11.3.3, "Indexing an Attribute"](#)

#### 3.11.3.1 Modifying the Directory Schema

First, you must prepare your LDIF file to define the new schema elements you want to add. See [Section A.3, "LDIF Format for Adding Schema Elements"](#) for examples. Once you have a properly formatted LDIF file, you can use the `ldapmodify` tool to import the new schema definitions into the directory schema.

##### Example:

```
ldapmodify -h myhost.company.com -D "cn=orcladmin" -q -p 3060 \
  -f /home/myfiles/modify.ldif -v
```

#### 3.11.3.2 Modifying an Entry

To modify the attributes or attribute values for an entry, you must first prepare your LDIF file correctly. See [Section A.2.3, "LDIF Format for Modifying Entries"](#) for examples. Once you have a properly formatted LDIF file, you can use the `ldapmodify` tool to import the changes.

##### Example:

```
ldapmodify -h myhost.company.com -D "cn=orcladmin" -q \
  -p 3060 -f /home/myfiles/modify.ldif -v
```

#### 3.11.3.3 Indexing an Attribute

You can add or drop an attribute in the catalog entry by using `ldapmodify`.

As of Oracle Internet Directory 11g Release 1 (11.1.1.6.0) a new autocatalog feature is enabled by default in fresh installs. You can also enable it if you have upgraded from a previous release. When this feature is enabled, Oracle Internet Directory automatically invokes the `catalog` command to index attributes when you search for them. If the autocatalog feature is not enabled, and you want to use previously uncataloged attributes in search filters, you must add them to the catalog entry, as in previous releases.

To add an attribute, import an LDIF file by using `ldapmodify`. For example, to index the attribute `displayName`, import the following LDIF file by using `ldapmodify`:

##### Example:

```
dn: cn=catalogs
```

```
changetype: modify
add: orclindexedattribute
orclindexedattribute: displayName
```

Type a command similar to the following at the system prompt:

```
ldapmodify -D "cn=orcladmin" -q -h host -p port -f ldif_file_name
```

To index the attribute, the `ldapmodify` command invokes the Catalog Management tool, `catalog`. For information about that tool, see [Section 3.4, "catalog."](#)

To drop an index from an attribute by using `ldapmodify`, specify `delete` in the LDIF file. For example:

```
dn: cn=catalogs
changetype: modify
delete: orclindexedattribute
orclindexedattribute: displayName
```

### 3.11.4 Related Command-Line Tools for ldapmodify

- See [Section 3.5, "ldapadd"](#)
- See [Section 3.9, "ldapdelete"](#)
- See [Section 3.10, "ldapmoddn"](#)

## 3.12 ldapmodifymt

The `ldapmodifymt` command-line tool is similar to `ldapmodify` in that it enables you to add, delete, or modify entries by supplying an LDIF file as input. However, `ldapmodifymt` runs in multi-threaded mode allowing you to operate on multiple entries concurrently.

See [Appendix A, "LDIF File Format"](#) for more information about the correct formatting of LDIF files.

### 3.12.1 Syntax for ldapmodifymt

```
ldapmodifymt -h oid_hostname -D "binddn" -q | -w password [-p ldap_port]
[-V ldap_version] -T number_of_threads {-f ldif_filename | -X dsml_filename}
[-a] [-b] [-c [-o log_file_name]] [-M] [-O ref_hop_limit]
[-U SSL_auth_mode {-W wallet_location -Q | -P wallet_password}]
[-E character_set] [-d debug_level]
```

### 3.12.2 Arguments for ldapmodifymt

#### **-h oid\_hostname**

Required. The host name or IP address of the Oracle Internet Directory server.

#### **-D "binddn"**

Required. The DN of the Oracle Internet Directory user needed to bind to the directory (for example, `cn=orcladmin`).

**-q**

Required unless `-w` is used. Causes the command to prompt for the user password needed to bind to the directory. A password supplied at the command prompt is not visible on the screen.

**-w password**

Required unless `-q` is used. The user password needed to bind to the directory. Avoid supplying a password on the command line whenever possible. A password typed on the command line is visible on your screen. The `-w password` option is disabled when `LDAP_PASSWORD_PROMPTONLY` is set to true. See [Section 1.1, "Using Passwords with Command-Line Tools."](#)

**-p ldap\_port**

Optional. The port number used to connect to the Oracle Internet Directory server. Defaults to port 3060.

**-V ldap\_version**

Optional. The version of the LDAP protocol to use. Allowed values are 2 or 3. Defaults to 3 (LDAP v3).

**-T number\_threads**

Required. The number of threads for concurrently processing entries.

**-f ldif\_filename | -X dsml\_filename**

Required. The full path and file name of the input file that contains the data you want to import.

Use the `-f` argument to supply an LDIF file. See [Appendix A, "LDIF File Format"](#) for information on formatting an LDIF file.

Use the `-x` argument to supply a Directory Service Markup Language (DSML) file. See [Section 3.5.3.2, "Adding Data to the Directory Using a DSML File"](#) for more information about formatting a DSML file.

**-a**

Optional. Denotes that the LDIF file has entries to be added.

**-b**

Optional. Use this option if your input file has binary file names in it, which are preceded by the forward slash character. The tool retrieves the actual values from the file referenced.

**-c**

Optional. Proceeds in spite of errors. All errors are reported. If the `-c` argument is not used, the tool stops when an error occurs.

**-o log\_file\_name**

Optional. Used with the `-c` argument. Writes the LDIF entries with errors to a log file. Specify the full path and name of the log file.

**-M**

Optional. Instructs the tool to send the `ManageDSAIT` control to the server. The `ManageDSAIT` control instructs the server not to send referrals to clients. Instead a referral entry is returned as a regular entry.

**-O ref\_hop\_limit**

Optional. The number of referral hops that a client should process. Defaults to 5.

**-U SSL\_auth\_mode**

Optional. The SSL authentication mode:

- 1 for no authentication required.
- 2 for one way authentication required. You must also supply a wallet location and wallet password.
- 3 for two way authentication required. You must also supply a wallet location and wallet password.

**-W wallet\_location**

Required if using one way or two way SSL authentication (`-U 2|3`). The location of the wallet file that contains the server's SSL certificates.

Example for UNIX:

```
-W "file:/home/my_dir/my_wallet"
```

Example for Microsoft Windows:

```
-W "file:C:\my_dir\my_wallet"
```

**-Q**

Required, unless `-P` is used, if using one way or two way SSL authentication (`-U 2|3`). Causes the command to prompt for the wallet password for the wallet specified in the `-W` argument. A password supplied at the command prompt is not visible on the screen.

**-P wallet\_password**

Required, unless `-Q` is used, if using one way or two way SSL authentication (`-U 2|3`). The wallet password for the wallet specified in the `-W` argument. Avoid supplying a password on the command line whenever possible. A password typed on the command line is visible on your screen. The `-P wallet_password` option is disabled when `LDAP_PASSWORD_PROMPTONLY` is set to true. See [Section 1.1, "Using Passwords with Command-Line Tools."](#)

**-E character\_set**

Optional. The native character set encoding. Defaults to the character set of the user's terminal. Each supported character set has a unique acronym, for example, `WE8MSWIN1252`, `JA16SJIS`, or `AL32UTF8`.

**-d debug\_level**

Optional. If not specified the default of 0 (not enabled) is used. Debug levels are additive. Add the numbers representing the functions that you want to activate, and use the sum of those in the command-line option. For example, to trace search filter processing (512) and active connection management (256), enter 768 as the debug level (512 + 256 = 768). Debug levels are as follows:

- 1 — Heavy trace debugging
- 128 — Debug packet handling
- 256 — Connection management, related to network activities
- 512 — Search filter processing
- 1024 — Entry parsing
- 2048 — Configuration file processing
- 8192 — Access control list processing
- 491520 — Log of communication with the database
- 524288 — Schema related operations
- 4194304 — Replication specific operations
- 8388608 — Log of entries, operations and results for each connection
- 16777216 — Trace function call arguments
- 67108864 — Number and identity of clients connected to this server
- 117440511 — All possible operations and data

### 3.12.3 Tasks and Examples for ldapmodifymt

Using the `ldapmodifymt` command-line tool, you can perform the following task:

- [Section 3.12.3.1, "Modifying Multiple Entries Concurrently"](#)

#### 3.12.3.1 Modifying Multiple Entries Concurrently

To modify multiple entries at once, you must first prepare your LDIF file correctly. See [Appendix A, "LDIF File Format"](#) for examples. Once you have a properly formatted LDIF file, you can use the `ldapmodifymt` tool to import the changes.

The following example uses five concurrent threads to modify the entries specified in the file `/home/myfiles/modify.ldif`.

**Example:**

```
ldapmodify -h myhost.company.com -D "cn=orcladmin" -w password -p 3060 \
-T 5 -f /home/myfiles/modify.ldif -v
```

### 3.12.4 Related Command-Line Tools for ldapmodifymt

- See [Section 3.6, "ldapaddmt"](#)
- See [Section 3.11, "ldapmodify"](#)

## 3.13 ldapsearch

The `ldapsearch` command-line tool enables you to search for and retrieve specific entries in the directory.

The LDAP filter that you use to search for entries must be compliant with the Internet Engineering Task Force (IETF) standards as specified in RFC 2254. Refer to the IETF Web site at <http://www.ietf.org> for more information about the standard filter format. Oracle Internet Directory supports all elements of RFC 2254 except for extensible matching.

---

---

**Note:** Various UNIX shells interpret some characters—for example, asterisks (\*)—as special characters. Depending on the shell you are using, you might need to escape these characters.

---

---

**See Also:** For information on using attribute aliases with ldapsearch refer to the "Attribute Aliases In the Directory" section in *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*

### 3.13.1 Syntax for ldapsearch

```
ldapsearch -h oid_hostname -D "binddn" -q | -w password [-Y "proxy_dn"]
[-p ldap_port] [-V ldap_version] -b "basedn" {-s base|one|sub} {"filter_string"
attributes}|-f input_file} [-F separator] [-T [-]sort_attribute] [-j page_size]
[-A] [-a never|always|search|find] [-S] [-R] [-i 1|0] [-t] [-u] [-L|-X] [-B] [-M]
[-v] [-n] [-l time_limit] [-z size_limit] [-O ref_hop_limit] [-U SSL_auth_mode
{-W wallet_location -Q | -P wallet_password}] [-d debug_level]
[-E character_set][-c]
```

### 3.13.2 Arguments for ldapsearch

**-h oid\_hostname**

Required. The host name or IP address of the Oracle Internet Directory server.

**-D "binddn"**

Required. The DN of the Oracle Internet Directory user needed to bind to the directory (for example, cn=orcladmin).

**-q**

Required unless `-w` is used. Causes the command to prompt for the user password needed to bind to the directory. A password supplied at the command prompt is not visible on the screen.

**-w password**

Required unless `-q` is used. The user password needed to bind to the directory. Avoid supplying a password on the command line whenever possible. A password typed on the command line is visible on your screen. The `-w password` option is disabled when `LDAP_PASSWORD_PROMPTONLY` is set to true. See [Section 1.1, "Using Passwords with Command-Line Tools."](#)

**-Y "proxy\_dn"**

Optional. The DN of a proxy user. After binding to the directory, the add operation is performed as this user.

**-p ldap\_port**

Optional. The port number used to connect to the Oracle Internet Directory server. Defaults to port 3060.

**-V ldap\_version**

Optional. The version of the LDAP protocol to use. Allowed values are 2 or 3. Defaults to 3 (LDAP v3).

**-b "basedn"**

Required. The base DN for the search.

**-s base | one | sub**

Required. The scope of the search within the DIT. The options are:

- `base` - Retrieves a particular directory entry. Along with this search depth, you use the search criteria bar to select the attribute `objectClass` and the filter `Present`.
- `one` - Limits your search to all entries beginning one level down from the root of your search.
- `sub` - Searches entries within the entire subtree, including the root of your search.

**"filter\_string" [attributes] | -f input\_file**

Required. Supply a single filter on the command-line within quotes followed by the attribute names whose values you want returned. Separate attributes with a space. If you do not list any attributes, all attributes are retrieved.

By default, `ldapsearch` does not return operational attributes. If you add the character "+" to the list of attributes in the search request, however, `ldapsearch` returns all operational attributes.

You can also supply an input file with the `-f` argument that contains a sequence of search operations to perform.

In the output, the attribute names are shown in lower case if the attribute `orclReqattrCase` is 0 in the instance-specific config entry. If `orclReqattrCase` is set to 1, the attribute names in the output are shown in the same case in which they were entered on the command line. See [Section 3.13.3.9, "Attribute Case in ldapsearch Output."](#)

**-F separator**

Optional. Enables you to choose a separator to use between attribute names and values in the search output. The default is = (equal sign).

**-T [-]sort\_attribute**

Optional. Instructs the tool to send a sort request to the server. The server returns entries sorted on the attribute, `sort_attribute`. A dash (-) before `sort_attribute` instructs the tool to sort the entries in reverse order.

**-j page\_size**

Optional. Instructs the tool to send a page request to the server. The server returns paged entries with pages of size, `page_size`.

**-A**

Optional. Retrieves attribute names only (no values).

**-a never | always | search | find**

Optional. Specifies alias dereferencing. An alias entry in an LDAP directory is an entry that points to another entry. Following an alias pointer is known as dereferencing an alias. The options are:

- `never` - Never dereference alias entries. Choose this option to improve search performance if there are no alias entries in the directory that require dereferencing.
- `always` - Always dereference aliases. This selection is the default.

- `search` - Dereference alias entries subordinate to a specified search base, but do not dereference an alias search base entry.
- `find` - Dereference an alias entry for a specified search base, but do not dereference alias entries subordinate to the search base.

**-S attr**

Optional. Sorts the results by the attribute specified.

**-R**

Optional. Disables the automatic following of referrals.

**-i 1 | 0**

Optional. Specifies whether to bind as the current user when following referrals. 1 means bind as the current user, 0 means bind anonymously. The default is 0 (zero).

**-t**

Optional. Writes files to `/tmp`.

**-u**

Optional. Includes user-friendly names in the output.

**-L | -X**

Optional. Prints entries in LDIF (`-L`) or DSML format (`-X`).

With the `-L` option, all attributes, including binary attributes are printed in LDAP Data Interchange Format (LDIF). Binary attributes are transformed into printable characters using BASE64 encoding.

**See Also:** [Appendix A, "LDIF File Format"](#) for a description of LDAP Data Interchange Format.

**-B**

Optional. Allows printing of non-ASCII values. Binary attributes are printed as is, without encoding. The complete value might not be printed, as it might contain non-printable characters.

**-M**

Optional. Instructs the tool to send the `ManageDSAIT` control to the server. The `ManageDSAIT` control instructs the server not to send referrals to clients. Instead a referral entry is returned as a regular entry.

**-n**

Optional. Enables you to preview what would occur in an operation without actually performing the operation.

**-v**

Optional. Runs the tool in verbose mode.

**-l time\_limit**

Optional. The maximum time in seconds to wait for an `ldapsearch` command to complete.



**-z size\_limit**

Optional. The maximum number of entries to return.

**-O ref\_hop\_limit**

Optional. The number of referral hops that a client should process. Defaults to 5.

**-U SSL\_auth\_mode**

Optional. The SSL authentication mode:

- 1 for no authentication required.
- 2 for one way authentication required. You must also supply a wallet location and wallet password.
- 3 for two way authentication required. You must also supply a wallet location and wallet password.

**-W wallet\_location**

Required if using one way or two way SSL authentication (-U 2|3). The location of the wallet file that contains the server's SSL certificates.

Example for UNIX:

```
-W "file:/home/my_dir/my_wallet"
```

Example for Microsoft Windows:

```
-W "file:C:\my_dir\my_wallet"
```

**-Q**

Required, unless -P is used, if using one way or two way SSL authentication (-U 2|3). Causes the command to prompt for the wallet password for the wallet specified in the -W argument. A password supplied at the command prompt is not visible on the screen.

**-P wallet\_password**

Required, unless -Q is used, if using one way or two way SSL authentication (-U 2|3). The wallet password for the wallet specified in the -W argument. Avoid supplying a password on the command line whenever possible. A password typed on the command line is visible on your screen. The -P *wallet\_password* option is disabled when LDAP\_PASSWORD\_PROMPTONLY is set to true. See [Section 1.1, "Using Passwords with Command-Line Tools."](#)

**-d debug\_level**

Optional. If not specified the default of 0 (not enabled) is used. Debug levels are additive. Add the numbers representing the functions that you want to activate, and use the sum of those in the command-line option. For example, to trace search filter processing (512) and active connection management (256), enter 768 as the debug level (512 + 256 = 768). Debug levels are as follows:

- 1 — Heavy trace debugging
- 128 — Debug packet handling
- 256 — Connection management, related to network activities
- 512 — Search filter processing
- 1024 — Entry parsing

- 2048 — Configuration file processing
- 8192 — Access control list processing
- 491520 — Log of communication with the database
- 524288 — Schema related operations
- 4194304 — Replication specific operations
- 8388608 — Log of entries, operations and results for each connection
- 16777216 — Trace function call arguments
- 67108864 — Number and identity of clients connected to this server
- 117440511 — All possible operations and data

**-E character\_set**

Optional. The native character set encoding. Defaults to the character set of the user's terminal. Each supported character set has a unique acronym, for example, WE8MSWIN1252, JA16SJIS, or AL32UTF8.

**-C**

Optional. ldapsearch -C option causes ldapsearch to traverse a hierarchy and report direct memberships. The ldapsearch -C option essentially includes the CONNECT\_BY control (2.16.840.1.113894.1.8.3) in the request sent to the client. ldapsearch doesn't have any means to pass values with a control. So, it sends the CONNECT\_BY control without values. In this case the default values are assumed, that is, the hierarchy-establishing attribute name is obtained from the filter, and the number of levels is 0. Thus, the -C option can only be used to fetch *all containers of a containee* queries, for example, fetch all groups of a user, fetch all employees of a manager and so forth. Also, all levels of the hierarchy are traversed. For more information, see [Section 6-2, "Request Controls Supported by Oracle Internet Directory."](#)

**See Also:** The "Performing Hierarchical Searches" section in Oracle Fusion Middleware Application Developer's Guide for Oracle Identity Management

### 3.13.3 Tasks and Examples for ldapsearch

Using the ldapsearch command-line tool, you can perform the following tasks:

- [Section 3.13.3.1, "Performing a Base Object Search"](#)
- [Section 3.13.3.2, "Performing a One-Level Search"](#)
- [Section 3.13.3.3, "Performing a Subtree Search"](#)
- [Section 3.13.3.4, "Searching for Attribute Values of Entries"](#)
- [Section 3.13.3.5, "Searching for Operational Attributes of Entries"](#)
- [Section 3.13.3.6, "Searching for Entries with Attribute Options"](#)
- [Section 3.13.3.7, "Searching for All User Attributes and Specified Operational Attributes"](#)
- [Section 3.13.3.8, "Searching for Entries \(More Examples\)"](#)
- [Section 3.13.3.9, "Attribute Case in ldapsearch Output"](#)

### 3.13.3.1 Performing a Base Object Search

The following example performs a base-level search on the directory from the root.

- `-b` specifies base DN for the search, root in this case.
- `-s` specifies whether the search is a base search (`base`), one level search (`one`) or subtree search (`sub`).
- `"objectclass=*"` specifies the filter for search.

#### Example:

```
ldapsearch -p 3060 -h myhost -b "" -s base -v "objectclass=*"
```

### 3.13.3.2 Performing a One-Level Search

The following example performs a one level search starting at `"ou=HR, ou=Americas, o=IMC, c=US"`.

#### Example:

```
ldapsearch -p 3060 -h myhost -b "ou=HR, ou=Americas, o=IMC, c=US" -s one \
-v "objectclass=*"
```

### 3.13.3.3 Performing a Subtree Search

The following example performs a subtree search and returns all entries having a DN starting with `"cn=us"`.

#### Example:

```
ldapsearch -p 3060 -h myhost -b "c=US" -s sub -v "cn=Person*"
```

### 3.13.3.4 Searching for Attribute Values of Entries

The following example returns only the DN attribute values of the matching entries:

#### Example:

```
ldapsearch -p 3060 -h myhost -b "c=US" -s sub -v "objectclass=*" dn
```

The following example retrieves only the distinguished name along with the surname (`sn`) and description (`description`) attribute values:

#### Example:

```
ldapsearch -p 3060 -h myhost -b "c=US" -s sub -v "cn=Person*" dn sn description
```

The following example retrieves the distinguished name (`dn`), surname (`sn`), and description (`description`) attribute values. The entries are sorted by surname (`sn`). There are 10 entries returned per page.

#### Example:

```
ldapsearch -p 3060 -h myhost -b "c=US" -s sub -v "cn=Person*" dn sn description \
-T sn -j 10
```

### 3.13.3.5 Searching for Operational Attributes of Entries

The following example returns only operational attributes:

```
$ ldapsearch -h adc2190517 -p 3060 -D cn=orcladmin -w welcome -b "c=uk" -L -s base
"(objectclass=*)" +
```

### 3.13.3.6 Searching for Entries with Attribute Options

The following example retrieves entries with common name (cn) attributes that have an option specifying a language code attribute option. This particular example retrieves entries in which the common names are in French and begin with the letter R.

**Example:**

```
ldapsearch -p 3060 -h myhost -b "c=US" -s sub "cn;lang-fr=R"
```

Suppose that, in the entry for John, no value is set for the cn;lang-it language code attribute option. In this case, the following example does not return John's entry:

**Example:**

```
ldapsearch -p 3060 -h myhost -b "c=us" -s sub "cn;lang-it=Giovanni"
```

### 3.13.3.7 Searching for All User Attributes and Specified Operational Attributes

The following example retrieves all user attributes and the createtimestamp and orclguid operational attributes:

**Example:**

```
ldapsearch -p 3060 -h myhost -b "ou=Benefits,ou=HR,ou=Americas,o=IMC,c=US" \
-s sub "cn=Person*" "*" createtimestamp orclguid
```

The following example retrieves entries modified by Anne Smith:

**Example:**

```
ldapsearch -h sun1 \
-b "" "(&(objectclass=*)(modifiersname=cn=Anne Smith))"
```

The following example retrieves entries modified between 01 April 2001 and 06 April 2001:

**Example:**

```
ldapsearch -h sun1 -b "" \
"(&(objectclass=*)(modifytimestamp >= 20000401000000) \
(modifytimestamp <= 20000406235959))"
```

---

**Note:** Because modifiersname and modifytimestamp are not indexed attributes, use catalog to index these two attributes. Then, restart the Oracle directory server before issuing the two previous ldapsearch commands.

---

### 3.13.3.8 Searching for Entries (More Examples)

Each of the following examples searches on port 3060 of host sun1, and searches the whole subtree starting from the DN "ou=hr,o=acme,c=us".

The following example searches for all entries with any value for the objectclass attribute.

```
ldapsearch -p 3060 -h sun1 -b "ou=hr, o=acme, c=us" -s subtree "objectclass=*
```

The following example searches for all entries that have orcl at the beginning of the value for the objectclass attribute.

```
ldapsearch -p 3060 -h sun1 -b "ou=hr, o=acme, c=us" -s subtree "objectclass=orcl*"
```

The following example searches for entries where the `objectclass` attribute begins with `orcl` and `cn` begins with `foo`.

```
ldapsearch -p 3060 -h sun1 -b "ou=hr, o=acme, c=us" \
-s subtree "(&(objectclass=orcl*)(cn=foo*))"
```

The following example searches for entries in which `cn` begins with `foo` or `sn` begins with `bar`.

```
ldapsearch -p 3060 -h sun1 -b "ou=hr, o=acme, c=us" \
-s subtree "(|(cn=foo*)(sn=bar*))"
```

The following example searches for entries in which `employeenumber` is less than or equal to 10000.

```
ldapsearch -p 3060 -h sun1 -b "ou=hr, o=acme, c=us" \
-s subtree "employeenumber<=10000"
```

### 3.13.3.9 Attribute Case in ldapsearch Output

In the output from the `ldapsearch` command, the attribute names are shown in lower case if the attribute `orclReqattrCase` in the instance-specific configuration entry is 0. If `orclReqattrCase` is set to 1, the attribute names in the output are shown in the same case in which they were entered on the command line.

Example:

```
ldapsearch -h localhost -p 389 -b "dc=oracle,dc=com" -s base -L "objectclass=" DC
```

If `orclReqattrCase` is 0 the output looks like this:

```
dn: dc=oracle,dc=comdc: oracle
```

If `orclReqattrCase` is 1, the output looks like this:

```
dn: dc=oracle,dc=comDC: oracle
```

## 3.13.4 Related Command-Line Tools for ldapsearch

- See [Section 3.8, "ldapcompare"](#)
- See [Section 3.4, "catalog"](#)

## 3.14 Idifmigrator

The Oracle Internet Directory Data Migration Tool (`ldifmigrator`) is used to convert LDIF files output from other directories or application-specific repositories into a format recognized by Oracle Internet Directory. The Data Migration Tool takes as input an LDIF file containing substitution variables, and outputs an LDIF file suitable for loading into Oracle Internet Directory.

See [Section A.4, "LDIF Format for Migrating Entries"](#) for the correct format of the LDIF input file for this tool.

### 3.14.1 Syntax for ldifmigrator

```
ldifmigrator "input_file=filename" "output_file=filename"
[-lookup -h oid_hostname "dn=binddn" -w password [-p ldap_port]
[subscriber=subscriberDN]] ["s_VariableName1=replacement_value"]
```

```
"s_VariableName2=replacement_value"...]
[-load -reconcile SAFE|SAFE_EXTENDED|NORMAL]
```

### 3.14.2 Arguments for ldifmigrator

**"input\_file=filename"**

The full path and file name of the LDIF file that contains directory entry data and one or more substitution variables.

**"output\_file=filename"**

The full path and file name of the output file produced by the ldifmigrator tool.

**-lookup**

If this flag is specified, then values of certain substitution variables are obtained by looking up the correct values in the directory server. See [Section A.4.1, "Substitution Variables for Migration Input Files"](#) for a list of substitution variables that can be looked up.

**-h oid\_hostname**

Required if the `-lookup` flag is used. The host name or IP address of the Oracle Internet Directory server.

**"dn= binddn"**

Required if the `-lookup` flag is used. The DN of the Oracle Internet Directory user needed to bind to the directory (for example, `cn=orcladmin`).

**-q**

Required unless `-w` is used. Causes the command to prompt for the user password needed to bind to the directory. A password supplied at the command prompt is not visible on the screen.

**-w password**

Required unless `-q` is used. The user password needed to bind to the directory. Avoid supplying a password on the command line whenever possible. A password typed on the command line is visible on your screen. The `-w password` option is disabled when `LDAP_PASSWORD_PROMPTONLY` is set to true. See [Section 1.1, "Using Passwords with Command-Line Tools."](#)

**subscriber=subscriberDN**

Optional. The subscriber whose attribute values is used in place of the substitution variables. If not specified, then the default identity management realm specified in the Root Oracle Context is used.

**"s\_VariableName=replacement\_value"**

Optional. You can specify a value for a substitution variable on the command-line. See [Section A.4.1, "Substitution Variables for Migration Input Files"](#) for instructions on adding a substitution variable to the input LDIF file. The ldifmigrator tool replaces all occurrences of the variable with the value you specify.

**-load**

Optional. Loads the data output by the `ldifmigrator` tool directly into Oracle Internet Directory. If an entry is already present in the directory then that directory entry is logged to the file. The addition of the directory entries could fail for other reasons as well, for instance not enough permission to add or parent entry not being present.

**-reconcile SAFE | SAFE\_EXTENDED | NORMAL**

Optional. The `-reconcile` option enables you to specify different modes if the tool tries to load data for entries that already exist, or modify attributes of entries that may have conflicts. The following modes are available:

- **SAFE** - This mode only adds new entries that don't exist or appends new attributes to existing entries.
- **SAFE-EXTENDED** - This mode only adds new entries that don't exist or appends new attributes to existing entries. If you try to add a new value for existing attributes, then it adds it to the existing set of values.
- **NORMAL** - This mode applies all directives as intended, overwriting any conflicting attributes or entries with the data specified in the `ldifmigrator` output.

See [Section A.4.2, "Reconcile Options for Migrated Entries"](#) for more information about LDIF directives supported by the `-reconcile` option.

### 3.14.3 Tasks and Examples for `ldifmigrator`

Using the `ldifmigrator` command-line tool, you can perform the following tasks:

- [Section 3.14.3.1, "Using the Data Migration Tool in Lookup Mode"](#)
- [Section 3.14.3.2, "Overriding Data Migration Values in Lookup Mode"](#)
- [Section 3.14.3.3, "Using the Data Migration Tool by Supplying Your Own Values"](#)
- [Section 3.14.3.4, "Loading and Reconciling Data Using the Data Migration Tool"](#)

See [Section A.4, "LDIF Format for Migrating Entries"](#) for examples of correctly formatted LDIF input files for use with the Data Migration Tool.

#### 3.14.3.1 Using the Data Migration Tool in Lookup Mode

In this example, Oracle Internet Directory server is present in the environment, and the migration tool looks up the directory server to figure out certain substitution variables specified in the LDIF input file.

**Example:**

```
$ldifmigrator "input_file=sample.dat" "output_file=sample.ldif" \
             -lookup "host=ldap.acme.com" "subscriber=acme" \
             "s_UserOrganization=Development"
```

#### 3.14.3.2 Overriding Data Migration Values in Lookup Mode

In some cases, you want to use the lookup mode but would also like to override the values of one or more of the pre-defined substitution variables. This can be done by specifying the override value in the command-line. The following command line shows how one can set the `UserNickNameAttribute` to `cn` overriding the default of `uid`:

**Example:**

```
$ldifmigrator "input_file=sample.dat" "output_file=sample.ldif" \
```

```
-lookup "host=ldap.acme.com" "subscriber=acme" \
"s_UserOrganization=Development" "s_UserNicknameAttribute=cn"
```

### 3.14.3.3 Using the Data Migration Tool by Supplying Your Own Values

The following example shows how you can specify your own values for substitution variables found in the LDIF input file, rather than using lookup mode.

**Example:**

```
$ldifmigrator "input_file=sample.dat" "output_file=sample.ldif" \
"s_UserContainerDN=cn=Users,o=Acme,dc=com" \
"s_UserNicknameAttribute=uid" "s_UserOrganization=Development"
```

### 3.14.3.4 Loading and Reconciling Data Using the Data Migration Tool

The Data Migration Tool gives you the option of loading the data directly into Oracle Internet Directory. Use the `-load` and `-reconcile` options to load data and safely reconcile any conflicts.

**Example:**

```
$ldifmigrator "input_file=sample.dat" "output_file=sample.ldif" \
-lookup "host=ldap.acme.com" "subscriber=acme" \
"s_UserOrganization=Development"
-load -reconcile SAFE
```

## 3.14.4 Related Command-Line Tools for ldifmigrator

- See Section 3.5, "ldapadd"
- See Section 3.11, "ldapmodify"
- See Section 3.15, "ldifwrite"

## 3.14.5 Error Messages for ldifmigrator

The Data Migration Tool can display these error messages:

**Table 3–1 Error Messages of the Data Migration Tool**

Message	Reason	Remedial Action
Environment variable ORACLE_HOME not defined	ORACLE_HOME is not defined.	Set the environment variable ORACLE_HOME
Environment variable ORACLE_INSTANCE not defined	ORACLE_INSTANCE is not defined.	Set the environment variable ORACLE_INSTANCE
Error while parsing the input parameters. Please verify	Not all the required parameters are provided. The required parameters are Input_File, Output_File and at least one substitution variable	Specify the input parameters properly. Use the <code>-help</code> option to print the usage.
Input_File parameter not specified. Please specify	Input_File parameter is a mandatory parameter.	Specify the input parameters properly. Use the <code>-help</code> option to print the usage.
Output_File parameter not specified. Please specify	Output_File parameter is a mandatory parameter.	Specify the input parameters properly. Use the <code>-help</code> option to print the usage.
The specified input file does not exist	The specified file location is invalid.	Check the input file path



**Table 3–1 (Cont.) Error Messages of the Data Migration Tool**

Message	Reason	Remedial Action
Check the input file. Zero byte input file	The input file does not contain any entries.	Provide a valid file with pseudo LDIF entries
Cannot create the output file. Output file already exists	The output file already exists	Check the Output_File flag
Access denied, cannot read from the input file	The specified input file does not have read permission	Check the read permission of the input file.
Access denied, cannot create the output file	You do not have permission to create the output file.	Check the permission of the directory under which the output file needs to be created.
Directory server name not specified. When -lookup option is used the host parameter should be specified	When the -lookup option is specified, the host parameter is mandatory.	Specify the host parameter.
Bind Dn parameter name not specified. When -lookup option is used the dn parameter should be specified	When the -lookup option is specified, the DN parameter is mandatory.	Specify the DN parameter.
The port number specified is invalid	The port number should be a numeric value.	Check the port number parameter
Unable to establish connection to directory. Please verify the input parameters: host, port, dn & password	The directory server may not be running on the specified host and port, or credentials may be invalid.	Check the host, port, DN and password parameters. Check <code>ORACLE_INSTANCE/diagnostics/logs/OID/tools/</code> .
Naming exception occurred while retrieving the subscriber information from the directory. Please verify the input parameters	The specified identity management realm does not exist in the directory	Check the realm parameter
Not all the substitution variables are defined in the directory server specified	If the identity management realm entry does not contain the required attributes, then this error occurs.	Check the realm entry in the directory
Error occurred while migrating LDIF data to Oracle Internet Directory	This might occur if something goes wrong in the middle of a process—for example, a failure of the directory server or disk.	Report the error message to the administrator

When an error condition occurs, the log messages are logged to this file:

`ORACLE_INSTANCE/ldap/install/LDIFMig_YYYY_MM_DD_HH_SS.log`.

### 3.15 ldifwrite

The `ldifwrite` command-line tool enables you to convert to LDIF all or part of the information residing in an Oracle Internet Directory. Once you have converted the information, you can load it into a new node in a replicated directory or another node for backup storage.

---

**Note:** The `ldifwrite` command requires that the environment variable `ORACLE_INSTANCE` be set.

---

---



---

**Note:** The `ldifwrite` tool output does not include operational data of the directory itself—for example, `cn=subschemasubentry`, `cn=catalogs`, and `cn=changelog` entries. To export these entries into LDIF format, use `ldapsearch` with the `-L` flag.

---



---

The `ldifwrite` tool performs a subtree search, including all entries below the specified DN, including the DN itself.

### Using Idifwrite with Replication

When you add data to a node that is part of a Directory Replication Group (DRG), you can use either bulk tools or LDAP tools, depending on the circumstances. The following rules apply:

- When you add new entries to all nodes in the DRG, you can use either bulk tools or LDAP tools. For more than 20K entries, bulk tools are significantly faster. If you use LDAP tools, add the entries to only one node in the DRG and let replication propagate the entries. If you use bulk tools, generate the intermediate file only once from the LDIF file and use that intermediate file to load the entries onto all the nodes in the DRG.
- When you copy existing entries from one node to another in the same replication group, use bulk tools. Use the `bulkload` option `restore=true` when you upload the data.
- If the LDIF file contains operational attributes, which it does when created with `ldifwrite`, use `bulkload` to add the entries.
- If the replication agreement is a partial replication agreement, use `ldifwrite` with the base DN as the replication agreement DN to write the entries to the LDIF file. Then use `bulkload` with the `restore=true` option to load the data.

### 3.15.1 Syntax for Idifwrite

```
ldifwrite connect=connect_string basedn=Base_DN ldiffile=LDIF_Filename
[filter=LDAP_Filter] [threads=num_of_threads] [debug="TRUE"|"FALSE"]
[encode=character_set] [verbose="TRUE"|"FALSE"]
```

### 3.15.2 Arguments for Idifwrite

#### **connect**

Required. The directory database connect string. If you already have a `tnsnames.ora` file configured, then this is the net service name specified in that file, which is located by default in `ORACLE_INSTANCE/config`. (You can set the `TNS_ADMIN` environment variable if you want to use a different location.)

#### **basedn**

Required. The base DN of the subtree to be written out in LDIF format.

If the base DN is a replication agreement entry, then you can back up part of the naming context based on the LDAP naming context configuration. Specify the replication agreement DN in this case.

#### **ldiffile**

Required. The full path and file name of the output LDIF file.

**filter**

Optional. This is the LDAP filter to be used. You can specify a filter to select entries that match a particular criteria. Only these entries would be written to the LDIF file.

**threads**

Optional. The number of threads used to read from the directory store and write to the LDIF output file. The default is the number of CPUs plus one.

**debug**

Optional. The debug option reports the logging level. This is useful in case the command runs into errors. The output is logged to the `ldifwrite.log` file. This file can be found under `ORACLE_INSTANCE/diagnostics/logs/OID/tools`.

**encode**

Optional. The native character set encoding. Defaults to the character set of the user's terminal. Each supported character set has a unique acronym, for example, `WE8MSWIN1252`, `JA16SJIS`, or `AL32UTF8`.

**verbose**

### 3.15.3 Tasks and Examples for ldifwrite

Using the `ldifwrite` command-line tool, you can perform the following tasks

- [Section 3.15.3.1, "Converting All Entries under a Naming Context to an LDIF File"](#)
- [Section 3.15.3.2, "Converting a Partial Naming Context to an LDIF File"](#)
- [Section 3.15.3.3, "Converting Entries that Match Criteria to an LDIF File"](#)

#### 3.15.3.1 Converting All Entries under a Naming Context to an LDIF File

The following example writes all the entries under `ou=Europe, o=imc, c=us` into the `output1.ldif` file.

The LDIF file and the intermediate file are always written to the current directory.

The `ldifwrite` tool includes the operational attributes of each entry in the directory, including `createtimestamp`, `creatorsname`, and `orclguid`.

When prompted for the Oracle Internet Directory password, enter the password of the ODS database user account.

**Example:**

```
ldifwrite connect="nldap" basedn="ou=Europe, o=imc, c=us" ldiffile="output1.ldif"
```

#### 3.15.3.2 Converting a Partial Naming Context to an LDIF File

The following example uses the following naming context objects defined in partial replication:

```
dn: cn=includednamingcontext000001, cn=replication namecontext,
orclagreementid=000001, orclreplicaid=node replica identifier, cn=replication
configuration
orclincludednamingcontexts: c=us
orclxcludednamingcontexts: ou=Americas, c=us
orclxcludedattributes: userpassword
objectclass: top
objectclass: orclreplnamectxconfig
```

In this example, all entries under `c=us` are backed up except `ou=Americas,c=us`. The `userpassword` attribute is also excluded.

**Example:**

```
ldifwrite connect="nldap" basedn="cn=includednamingcontext000001, \
cn=replication namecontext,orclagreementid=000001, \
orclreplicaid=node replica identifier,cn=replication configuration" \
ldiffile="output2.ldif"
```

### 3.15.3.3 Converting Entries that Match Criteria to an LDIF File

The following example writes entries under `ou=users,o=test,c=us` that have `sn="Stuart"` to an output LDIF file, `output3.ldif`.

**Example:**

```
ldifwrite connect="nldap" basedn="ou=users, o= test, c=us" filter="sn=xyz"
ldiffile="output3.ldif"
```

## 3.15.4 Related Command-Line Tools for `ldifwrite`

- [Section 3.13, "ldapsearch"](#)
- [Section 3.14, "ldifmigrator"](#)
- [Section 3.2, "bulkload"](#)

## 3.16 upgradecert.pl

Starting with Release 10.1.2, a certificate hash value can be used to bind to Oracle Internet Directory. The introduction of this hash value requires that user certificates issued before Release 10.1.2 be updated in the directory. This is a post-upgrade step and it is required only if user certificates are provisioned in the directory. The `upgradecert.pl` tool is used for this purpose.

Before running the `upgradecert.pl` tool:

1. Make sure that the Oracle Internet Directory server instance is up and running.
2. Check that you are running Perl 5.6 or later. Run this command:  

```
perl -version
```
3. Make sure that the environment variable `PERL5LIB` is set to the proper PERL library location.
4. Check that you can run `ldapmodify` and `ldapsearch` from your command prompt.
5. Determine whether you have enough disk space to run the tool. The amount of disk space required depends upon the number of certificates stored.

### 3.16.1 Syntax for `upgradecert.pl`

```
perl ORACLE_HOME/ldap/bin/upgradecert.pl -h oid_hostname -D "binddn"
-w password [-p ldap_port] [-t temp_dir]
```

## 3.16.2 Arguments for upgradecert.pl

### **-h oid\_hostname**

Required. The host name or IP address of the Oracle Internet Directory server.

### **-D "binddn"**

Required. The DN of the Oracle Internet Directory user needed to bind to the directory (for example, cn=orcladmin).

### **-q**

Required unless `-w` is used. Causes the command to prompt for the user password needed to bind to the directory. A password supplied at the command prompt is not visible on the screen.

### **-w password**

Required unless `-q` is used. The user password needed to bind to the directory. Avoid supplying a password on the command line whenever possible. A password typed on the command line is visible on your screen. The `-w password` option is disabled when `LDAP_PASSWORD_PROMPTONLY` is set to true. See [Section 1.1, "Using Passwords with Command-Line Tools."](#)

### **-t temp\_dir**

Optional. The location of the temporary working directory. This is where the log file is found. The default is `$ORACLE_INSTANCE/diagnostics/logs/OID/tools` if the `ORACLE_INSTANCE` environment variable is set. If this variable is not set, the default is the current directory.

## 3.16.3 Tasks and Examples for upgradecert.pl

Using the `upgradecert.pl` tool, you can perform the following task:

- [Section 3.16.3.1, "Upgrading User Certificates Stored in the Directory from Releases Prior to 10.1.2"](#)

### 3.16.3.1 Upgrading User Certificates Stored in the Directory from Releases Prior to 10.1.2

#### **Example:**

```
perl ORACLE_HOME/ldap/bin/upgradecert.pl -h myhost.company.com \  
-D "cn=orcladmin" -w password
```

## 3.16.4 Related Command-Line Tools for upgradecert.pl

- N/A



---

---

# Oracle Internet Directory Replication Management Tools

This chapter describes the command-line tools used to administer Oracle Internet Directory replication.

This chapter includes the following sections:

- [Section 4.1, "ManageHiq.retry and ManageHiq.purge"](#) (Human Intervention Queue Management Tools)
- [Section 4.2, "oidcmprec"](#) (Oracle Internet Directory Compare and Reconcile Tool)
- [Section 4.3, "remtool"](#) (Replication Environment Management Tool)

---

---

**See Also:** The replication chapters in *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*.

---

---

## 4.1 ManageHiq.retry and ManageHiq.purge

When a replication conflict arises, the Oracle Internet Directory replication server places the change in the retry queue and tries to apply it from there for a specified number of times. If it fails after the specified number of retries, the replication server puts the change in the human intervention queue. From there, the replication server repeats the change application process at less frequent intervals while awaiting your action.

At this point, you must:

1. Examine the change in the human intervention queue.
2. Reconcile the conflicting changes using the Compare and Reconcile Tool (see [Section 4.2, "oidcmprec."](#))
3. Either place the change back into the retry queue, by using `ManageHiq.retry`, or into the purge queue, by using `ManageHiq.purge`.

---

---

**Note:** The Oracle Internet Directory server parameter `orclSizeLimit`, which is 1000 by default, limits the number of entries that the human intervention queue manipulation tools can process. If you have more than 1000 entries in the human intervention queue, you must increase `orclSizeLimit`, or some entries will never be processed. Setting the parameter `orclSizeLimit` very high impacts server performance, because `orclSizeLimit` also controls the maximum number of entries to be returned by a search. The DN containing `orclSizeLimit` is

```
cn=componentname,cn=osldldapd,cn=subconfigsentry
```

---

---

### 4.1.1 Syntax for ManageHiq.retry and ManageHiq.purge

You invoke `ManageHiq.retry` and `ManageHiq.purge` as PL/SQL commands at the SQL prompt, as follows:

```
$ sqlplus /nologSQL> connect ods;
SQL> Enter password
SQL> Set serveroutput ON
SQL> exec ManageHiq.retry(SupplierNode, EqualChgNo, StartChgNo, EndChgNo)
SQL> exit
```

```
$ sqlplus /nologSQL> connect ods;
SQL> Enter password
SQL> Set serveroutput ON
SQL> exec (ManageHiq.purgeSupplierNode, EqualChgNo, StartChgNo, EndChgNo)
SQL> exit
```

You must set server output ON to display the success or error message. The arguments are:

*EqualChgNo*—The change number to be moved to the retry queue.

*StartChgNo*—The starting number. All the change numbers after this should be moved to the retry queue.

*EndChgNo*—The ending change. All change numbers less than or equal to this change number that should be moved to the retry queue.

### 4.1.2 Examples for ManageHiq.retry

Move the changelog on node1, for change numbers between 300 and 1000 and supplier node2, to the retry queue.

```
exec Managehiq.retry('node2_orcl', 0, 300, 1000)
```

Move all the changelogs on node1 for supplier node2\_orcl to the retry queue.

```
exec Managehiq.retry('node2_orcl', 0, 0, 0)
```

or

```
exec Managehiq.retry('node2_orcl')
```

### 4.1.3 Examples for ManageHiq.purge

Purge the changelog on node1 where the change number is 2152 and the supplier is node2 (supplierNode = node2\_orcl)



```
exec Managehiq.purge('node2_orcl', 2152)
```

Purge the changelog on node1 where the change number is greater than 200 and the supplier is node2\_orcl

```
exec Managehiq.purge('node2_orcl', 0, 200)
```

Or

```
exec Managehiq.purge('node2_orcl', 0, 200, 0)
```

Purge the changelog on node1 where the change number is less than 2000 and the supplier is node2\_orcl

```
exec Managehiq.purge('node2_orcl', 0, 0, 2000)
```

## 4.2 oidcmprec

The Compare and Reconcile Tool allows you to compare one Oracle Internet Directory with another, detect conflicts or discrepancies, and optionally resolve them. The directories being compared can be standalone directories or part of the same replication group. You can compare two individual entries, subtrees, or entire directories. You can also compare directory schema. For more information, see "Comparing and Reconciling Inconsistent Data by Using oidcmprec" in *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*.

---

**Note:** The oidcmprec 11g tool supports data migration from 10g to 11g. However, data migration is not supported from 11g to 10g.

---

The oidcmprec tool can detect and resolve the following conflict scenarios:

- Entry only in source directory (entos)
- Entry only in destination directory (entod)
- Attribute only in source directory (atros)
- Attribute only in destination directory (atrod)
- Single-valued attribute differs (svatrdif)
- Multi-valued attribute differs (mvatrdif)
- Entry DN differs (dndif)

The oidcmprec tool can also detect and resolve the following schema conflict scenarios:

- Object class definition exists only in source directory (odefos)
- Object class definition exists only in destination directory (odefod)
- Object class definition different in source and destination directory (odefdif)
- Attribute definition exists only in source directory (adefos)
- Attribute definition exists only in destination directory (adefod)
- Attribute definition different in source and destination directory (adefdif)

### 4.2.1 Syntax for oidcmprec

```
oidcmprec operation=compare | reconcile | merge | merge_dryrun | userdefinedcr
```

```

source=host:port
destination=host:port
base="'dn1' 'dn2' 'dn3' ..."
[ ssslport=true | false ]
[ dsslport=true | false ]
[ dns2exclude="'edn1' 'edn2' 'edn3' ..." ]
[ scope=base | subtree | onelevel ]
[ filter=filter_that_conforms_to_RFC_2254 ]
[ threads=number_of_worker_threads ]
[ dnthreads=number_of_dn_threads ]
[ exclattr=space_separated_list_of_attributes_to_be_excluded |
  inclattr=space_separated_list_of_attributes_to_be_included ]
[ compareby=tool | ldapserver ]
[ filename=file_name_without_extension_to_store_compare_report ]
[ genchglog=d[efault] | t[rue] | f[alse] ]
[ reconaver=t[rue] | f[alse] ]
[ verbose=t[rue] | f[alse] ]
[ force=t[rue] | f[alse] ]
[ contonerr = t[rue] | f[alse] ]
[ logrpt = t[rue] | f[alse] ]
[ logs2d = t[rue] | f[alse] ]
[ logd2s = t[rue] | f[alse] ]
[ logeos = t[rue] | f[alse] ]
[ logeod = t[rue] | f[alse] ]
[ logdif = t[rue] | f[alse] ]
[ logerr = t[rue] | f[alse] ]
[ qlogfreq=frequency ]
[ help=t[rue] | f[alse] ]
sbinddn='("dn")'
dbinddn='("dn")'
[schemafilename=<Schema_filename for compare/merge/userdefinedcr against
destination schema>]
[ entos=ignore | add | del | log2add | log2del | log ]
[ entod=ignore | add | del | log2add | log2del | log ]
[ atos=ignore | add | del | log2add | log2del | usenewer |
  log2usenewer | useolder | log2useolder | usesmallguid |
  log2usesmallguid | usebigguid | log2usebigguid | log ]
[ atrod=ignore | add | del | log2add | log2del | usenewer |
  log2usenewer | useolder | log2useolder | usesmallguid |
  log2usesmallguid | usebigguid | log2usebigguid | log ]
[ svatrdif=ignore | usesrc | log2usesrc | usedest | log2usedest |
  usenewer | log2usenewer | useolder | log2useolder |
  usesmallguid | log2usesmallguid | usebigguid | log2usebigguid
  | log ]
[ mvatrdif=ignore | usesrc | log2usesrc | usedest | log2usedest | merge
  | log2merge | usenewer | log2usenewer | useolder |
  log2useolder | usesmallguid | log2usesmallguid | usebigguid |
  log2usebigguid | log ]
[ dndif=ignore | usesrc | log2usesrc | usedest | log2usedest | log ]
[ odefos=ignore | add | log2add | del | log2del | log ]
[ odefod=ignore | add | log2add | del | log2del | log ]
[ odefdif=ignore | usesrc | log2usesrc | usedest | log2usedest | merge |
  log2merge | log ]
[ adefos=ignore | add | log2add | del | log2del | log ]
[ adefod=ignore | add | log2add | del | log2del | log ]
[ adefdif=ignore | usesrc | log2usesrc | usedest | log2usedest | log ]
oidcmprec paramfile=file_containing_parameters]
oidcmprec [ xmlparamfile=file_containing_parameters_in_XML_format]

```

## 4.2.2 Arguments for oidcmprec

### **operation=compare | reconcile | merge | merge\_dryrun | userdefinedcr**

Required. The operation to perform. The operation argument can take the following values:

- `compare`: Compares the two directories, reports conflicts, and logs the changes that must be applied to the destination directory to resolve conflicts.
- `reconcile`: Compares the two directories, resolves conflicts, and logs the changes applied to the destination directory to resolve conflicts.
- `merge`: Compares the two directories and synchronizes them, updates both the source and destination directories. The source directory wins in case of a conflict.
- `merge_dryrun`: Performs a dry run of the merge operation. Logs all changes that must be made to synchronize the source and destination directories.
- `userdefinedcr`: Performs a user-defined `compare` and `reconcile` operation. Allows the user to choose the conflict resolution rules.

By default, the `oidcmprec` tool excludes operational attributes during comparison. That is, `oidcmprec` does not compare the operational attributes values in source and destination directory entries. During reconciliation of user defined attributes however, operational attributes might be changed.

### **source=host:port**

Required. The connection string used to bind to the source Oracle Internet Directory node. You are prompted for the replication DN password. If you do not supply the hostname or port information on the command-line, the tool prompts you for the information. The connection string is composed of the following elements:

- The host name of the directory server that acts as the source directory
- The LDAP listening port of the directory server

### **destination=host:port**

Required. The connection string used to bind to the source Oracle Internet Directory node. You are prompted for the replication DN password. If you do not supply the hostname or port information on the command-line, the tool prompts you for the information. The connection string is composed of the following elements:

- The host name of the directory server that acts as the destination directory
- The LDAP listening port of the directory server

### **base=" 'dn1' 'dn2' 'dn3'..."**

Required. Specifies the Distinguished Names (DNs) from where the comparison operation begins. The `scope` argument determines if child entries and subtrees of the base DN would be compared as well.

### **ssslport=true | false**

Optional. Specifies whether the source directory port is SSL or not. The default value is `false`. To specify this in an XML parameter file, use the `isSSLPort` parameter. See the example in [Section 4.2.3.10, "Using a Parameter File in XML Format."](#)

**dsslport=true | false**

Optional. Specifies whether the destination port is SSL or not. The default value is `false`. To specify this in an XML parameter file, use the `isSSLPort` parameter. See the example in [Section 4.2.3.10, "Using a Parameter File in XML Format."](#)

**dns2exclude=" 'edn1' 'edn2' 'edn3'..."**

Optional. Specifies DNs that are to be excluded from the comparison operation. These DNs must be child entries or subtrees of the DNs specified in the `base` argument.

**scope=base | subtree | onelevel**

Optional. Specifies whether the child entries and subtrees of a base DN are also compared. The `scope` argument can take the following values:

- `base`: Only the DNs specified in the `base` argument are compared. This is the default value.
- `subtree`: Directory information trees (DITs) identified by the DNs specified in the `base` argument are compared.
- `onelevel`: Only the immediate children of the DNs specified in the `base` argument are compared.

**filter=filter\_that\_conforms\_to\_RFC\_2254**

Optional. Only the entries that match the filter conditions are compared. The filter must be in the same format you would specify for `ldapsearch`. That is, it must conform to RFC 2254.

**threads=number\_of\_worker\_threads**

Optional. Specifies the number of worker threads that should be created. Worker threads are responsible for comparing entries, and reconciling the differences. One worker thread is created, by default.

If the `scope` is `base`, then the `threads` argument is ignored and it spawns one worker thread and one DN thread.

**dnthreads=number\_of\_dn\_threads**

Optional. Specifies the number of DN threads that should be created. DN threads are responsible for collecting all DNs that must be compared.

One DN thread is created, by default. The total number of DN threads and worker threads cannot exceed "`6 * Number of CPUs - 2`". If the total number of DN threads and worker threads exceeds the maximum value, the tool reduces both values proportionately to "`6 * Number of CPUs - 2`".

**exclattr=space\_separated\_list\_of\_attributes\_to\_be\_excluded |****inclattr=space\_separated\_list\_of\_attributes\_to\_be\_included**

Optional. Specifies the list of attributes to be excluded or included for comparison. You can either specify a list of attributes to be excluded, using `exclattr`, or specify a list of attributes to be included, using `inclattr`.

All attributes are included by default, except the following operational attributes:

- `creatorsname`
- `createtimestamp`
- `modifiersname`

- modifytimestamp
- orclentrydn
- orclnormdn

---



---

**Notes:**

- The `exclattr` and `inclattr` attributes cannot be used together, except when you use "\*" for `inclattr`.
  - By default, the `oidcmprec` tool excludes operational attributes during comparison. That is, `oidcmprec` does not compare the operational attributes values in source and destination directory entries. During reconciliation of user defined attributes however, operational attributes might be changed.
- 
- 

The option allows limited pattern matching. You can use `attributename*` to match all attributes starting with `attributename`. You can also use `attributename;*` to match all subtypes of `attributename`.

**compareby=tool | ldapserver**

Optional. Specifies whether the `compare` operation is performed by the `tool` or `ldapserver`. A `compare` operation performed by the `tool` is several times faster than a `compare` operation performed by `ldapserver`. The default value is `tool`.

**filename=file\_name**

Optional. Specifies a base name for the report files that would be generated by the tool. Do not specify an extension with the file name. The tool generates the following files:

- `file_name.rpt`: This file contains the DNs of all entries compared and the compare results. This file is known as the `rpt` file.
- `file_name.s2d.ldif`: This file contains all changes that were applied (or to be applied) to the destination directory. `s2d` stands for source directory to destination directory. This file is known as the `s2d` file.
- `file_name.d2s.ldif`: This file contains all changes that were applied (or to be applied) to the source directory. `d2s` stands for destination directory to source directory. This file is known as the `d2s` file.
- `file_name.eos.rpt`: This file lists DNs of entries that exist only in the source directory. `eos` stands for entries available only in the source directory. This file is known as the `eos` file.
- `file_name.eod.rpt`: This file lists DNs of entries that exist only in the destination directory. `eod` stands for entries available only in the destination directory. This file is known as the `eod` file.
- `file_name.dif.rpt`: This file lists the DNs that are different in the source and destination directories along with the names of the DN attributes that differ. This file is known as the `dif` file.
- `file_name.err`: This file contains all the error messages. It is known as the `err` file.

**genchglog=d[default] | t[true] | f[false]**

Optional. Determines whether a change log is created for the changes made by the `oidcmprec` tool. The `genchglog` argument can have the following values:

- `default`: The OID server settings decide whether a change log is generated or not. Change logs are generated if the root entry's `orclidprepository` attribute is set to `true`. A value of `false` means that change logs are not generated. The same rule applies for both the source and destination directories. `default` is the default value for `genchglog`.
- `true`: Change logs are always generated irrespective of the settings on the source and destination directories.
- `false`: Change logs are never generated irrespective of the settings on the source and destination directories.

**reconaver=t[true] | f[false]**

Optional. Determines whether attribute version reconciliation support is provided. The default value is `false`. Source and destination directory versions must be greater than 11.1.1.0.0 or directories must have the appropriate patch.

**verbose=t[true] | f[false]**

Optional. Determines whether the `rpt` file is shown on the screen. The default value is `false`. When set to `true`, `verbose` displays the report file on the screen as it is generated. When `verbose` is set to `false`, the tool shows its progress on the screen by displaying the count of entries it has processed.

**force=t[true] | f[false]**

Optional. Determines whether the tool prompts the user for confirmation before performing the specified operation. The default value is `false`. When set to `true`, the tool does not prompt the user for confirmation before performing the specified operation.

**contonerr=t[true] | f[false]**

Optional. Determines whether the tool shall continue when it encounters an error. The `contonerr` argument can have the following values:

- `true`: The tool continues to process other entries even if there is an error. This is the default value for `contonerr`.
- `false`: The tool stops if it encounters an error.

---

**Note:** If the tool encounters a critical error, it stops irrespective of the value passed to `contonerr`.

---

**logrpt=t[true] | f[false]**

Optional. Controls whether the tool generates the `file_name.rpt` file. The `logrpt` argument can have the following values:

- `true`: The tool generates the file. This is the default.
- `false`: The tool does not generate the file.

**logs2d=t[true] | f[false]**

Optional. Controls whether the tool generates the *file\_name.s2d.ldif* file. The logs2d argument can have the following values:

- true: The tool generates the file. This is the default.
- false: The tool does not generate the file.

**logd2s=t[true] | f[false]**

Optional. Controls whether the tool generates the *file\_name.d2s.ldif* file. The logd2s argument can have the following values:

- true: The tool generates the file. This is the default.
- false: The tool does not generate the file.

**logeos=t[true] | f[false]**

Optional. Controls whether the tool generates the *file\_name.eos.rpt* file. The logeos argument can have the following values:

- true: The tool generates the file. This is the default.
- false: The tool does not generate the file.

**logeod=t[true] | f[false]**

Optional. Controls whether the tool generates the *file\_name.eod.rpt* file. The logeod argument can have the following values:

- true: The tool generates the file. This is the default.
- false: The tool does not generate the file.

**logdif=t[true] | f[false]**

Optional. Controls whether the tool generates the *file\_name.dif.rpt* file. The logdif argument can have the following values:

- true: The tool generates the file. This is the default.
- false: The tool does not generate the file.

**logerr=t[true] | f[false]**

Optional. Controls whether the tool generates the *file\_name.err* file. The logdif argument can have the following values:

- true: The tool generates the file. This is the default.
- false: The tool does not generate the file.

**qlogfreq=frequency**

Optional. The tool can dump the total number of entries loaded by the tool in memory and the number of entries in each of oidcmprec's various queues. The entry counts are logged in the file *oidcmprec.log*. Use the qlogfreq argument to specify how frequently oidcmprec logs this information. Possible values are from 1 to 5000. The lower the value, the shorter the interval. For frequent entry counts, use a value between 5 and 10.

**help=t[true] | f[false]**

Optional. When set to true, the tool displays help on the oidcmprec command. The default value is false.

**sbinddn='("dn")'**

Optional. Specifies the DN to bind with the source directory. This argument is used if Oracle Virtual Directory is the source.

**dbinddn='("dn")'**

Optional. Specifies the DN to bind with the destination directory. This argument is used if Oracle Virtual Directory is the destination.

**entos=ignore | add | del | log2add | log2del | log**

Optional. Specifies the conflict resolution rule to use in case an entry exists only in the source directory. The following values are allowed:

- ignore: Ignore the conflict and take no action
- add: Add the entry to the peer directory
- del: Delete the entry from the directory
- log2add: Same as add except that the change is logged to an LDIF file and not directly effected in the peer directory
- log2del: Same as del except that the change is logged to an LDIF file and not directly effected in the directory
- log: Log the conflict in the report file and take no other action

The default value depends on the operation specified. [Table 4–1](#) shows the default values of the entos argument, corresponding to the operations specified.

**Table 4–1 Default Values for the entos Argument**

Operation	Default Value
compare	log2add
reconcile	add
merge	add
merge_dryrun	log2add
userdefinedcr	ignore

**entod=ignore | add | del | log2add | log2del | log**

Optional. Specifies the conflict resolution rule to use in case an entry exists only in the destination directory. The values allowed are the same as the entos argument.

The default value depends on the operation specified. [Table 4–2](#) shows the default values of the entod argument, corresponding to the operations specified.

**Table 4–2 Default Values for the entod Argument**

Operation	Default Value
compare	log2delete
reconcile	delete
merge	add
merge_dryrun	log2add
userdefinedcr	ignore



**atros=ignore | add | del | log2add | log2del | usenewer | log2usenewer | useolder | log2useolder | usesmallguid | log2usesmallguid | usebigguid | log2usebigguid | log**

Optional. Specifies the conflict resolution rule to use in case an attribute exists only in the source directory. The following values are allowed:

- ignore: Ignore the conflict and take no action
- add: Add the attribute to the corresponding entry in the peer directory
- del: Delete the attribute from the directory
- log2add: Same as add, except that the change is logged into an LDIF file and not directly effected in the peer directory.
- log2del: Same as del except that the change is logged into an LDIF file and not directly effected in the directory.
- usenewer: Check the `modifytimestamp` value to determine if the attribute should be deleted from the directory or added to the peer directory. The directory with the newer `modifytimestamp` value wins. If the `modifytimestamp` values are the same, then the source directory wins.
- log2usenewer: Same as usenewer except that the change is logged into an LDIF file and not directly effected in the directory.
- useolder: Check the `modifytimestamp` value to determine if the attribute should be deleted from the directory or added to the peer directory. The directory with the older `modifytimestamp` value wins. If the `modifytimestamp` values are the same, then the source directory wins.
- log2useolder: Same as useolder except that the change is logged to an LDIF file and not directly effected in the directory.
- usesmallguid: Check the GUID value to determine if the attribute should be deleted from the directory or added to the peer directory. The directory with the smaller GUID value wins. The GUID values would be the same in the same replication group. This rule is intended for non replication environments. If the GUID values are the same in both directories, then the source directory wins.
- log2usesmallguid: Same as usesmallguid except that the change is logged into an LDIF file and not directly effected in the directory.
- usebigguid: Check the GUID value to determine if the attribute should be deleted from the directory or added to the peer directory. The directory with the bigger GUID value wins. The GUID values would be the same in the same replication group. This rule is intended for non replication environments. If the GUID values are the same in both directories, then the source directory wins.
- log2usebigguid: Same as usebigguid except that the change is logged into an LDIF file and not directly effected in the directory.
- log: Log the conflict in the report file and take no other action.

The default value depends on the operation specified. [Table 4–3](#) shows the default values of the `atros` argument, corresponding to the operations specified.

**Table 4–3 Default Values for the `atros` Argument**

Operation	Default Value
compare	log2add
reconcile	add

**Table 4–3 (Cont.) Default Values for the atrod Argument**

Operation	Default Value
merge	add
merge_dryrun	log2add
userdefinedcr	ignore

**atrod=ignore | add | del | log2add | log2del | usenewer | log2usenewer | useolder | log2useolder | usesmallguid | log2usesmallguid | usebigguid | log2usebigguid | log**

Optional. Specifies the conflict resolution rule to use in case an attribute exists only in the destination directory. The values allowed are the same as the atrod argument.

The default value depends on the operation specified. Table 4–4 shows the default values of the atrod argument, corresponding to the operations specified.

**Table 4–4 Default Values for the atrod Argument**

Operation	Default Value
compare	log2delete
reconcile	delete
merge	add
merge_dryrun	log2add
userdefinedcr	ignore

**svatrdif=ignore | usesrc | log2usesrc | usedest | log2usedest | usenewer | log2usenewer | useolder | log2useolder | usesmallguid | log2usesmallguid | usebigguid | log2usebigguid | log**

Optional. Specifies the conflict resolution rule to use when a single-valued attribute for an entry is different in the two directories. The following values are allowed for the svatrdif argument:

- ignore: Ignore the conflict and take no action
- usesrc: Replace the value of the attribute in the destination directory with the value of the attribute in the source directory
- log2usesrc: Same as usesrc, except that the change is logged into an LDIF file and not directly effected in the destination directory
- usedest: Replace the value of the attribute in the source directory with the value of the attribute in the destination directory
- log2usedest: Same as usedest except that the change is logged into an LDIF file and not directly effected in the source directory
- usenewer: If the modifystamp value of the attribute in the source directory is newer than the destination directory, then update the attribute value in the destination directory. If the modifystamp value of the attribute in the destination directory is newer, then change the attribute value in the source directory. If the modifystamp values in both directories are the same, then the source directory wins.
- log2usenewer: Same as usenewer except that the change is logged into an LDIF file and not directly effected in the directory.

- **useolder**: If the `modifystamp` value of the attribute in the source directory is older than the destination directory, then update the attribute value in the destination directory. If the `modifystamp` value of the attribute in the destination directory is older, then change the attribute value in the source directory. If the `modifystamp` values in both directories are the same, then the source directory wins.
- **log2useolder**: Same as `useolder` except that the change is logged into an LDIF file and not directly effected in the directory.
- **usesmallguid**: If the source directory entry's GUID is smaller than the destination directory entry's GUID, then update the attribute in the destination directory. If the destination directory entry's GUID is smaller, then update the attribute in the source directory. If the GUID values are the same, then the source directory wins. This rule is meant for nonreplication environments, as the GUID values would be the same in the same replication group.
- **log2usesmallguid**: Same as `usesmallguid` except that the change is logged into an LDIF file and not directly effected in the directory.
- **usebigguid**: If the source directory entry's GUID is bigger than the destination directory entry's GUID, then update the attribute in the destination directory. If the destination directory entry's GUID is bigger, then update the attribute in the source directory. If the GUID values are the same, then the source directory wins. This rule is meant for nonreplication environments, as the GUID values would be the same in the same replication group.
- **log2usebigguid**: Same as `usebigguid` except that the change is logged into an LDIF file and not directly effected in the directory.
- **log**: Log the conflict in the report file and take no other action

The default value depends on the operation specified. [Table 4–5](#) shows the default values of the `svatrdif` argument, corresponding to the operations specified.

**Table 4–5** *Default Values for the `svatrdif` Argument*

Operation	Default Value
compare	log2usesrc
reconcile	usesrc
merge	usesrc
merge_dryrun	log2usesrc
userdefinedcr	ignore

**mvatrdif=ignore | usesrc | log2usesrc | usedest | log2usedest | merge | log2merge | usenewer | log2usenewer | useolder | log2useolder | usesmallguid | log2usesmallguid | usebigguid | log2usebigguid | log**

Optional. Specifies the conflict resolution rule to use when a multivalued attribute for an entry is different in the two directories. The values allowed are the same as the `svatrdif` argument. This argument also has other values that do not exist for the `svatrdif` argument. The following are values specific to the `mvatrdif` argument:

- **merge**: The missing attribute values in the destination directory are added from the source directory and those missing in the source directory are added from the destination directory.
- **log2merge**: Same as `merge` except that the changes are logged into an LDIF file and not directly effected in the directory.

The default value depends on the operation specified. [Table 4–6](#) shows the default values of the `mvatrdif` argument, corresponding to the operations specified.

**Table 4–6 Default Values for the `mvatrdif` Argument**

Operation	Default Value
compare	log2usesrc
reconcile	usesrc
merge	merge
merge_dryrun	log2merge
userdefinedcr	ignore

**`dndif=ignore | usesrc | log2usesrc | usedest | log2usedest | log`**

Optional. Specifies the conflict resolution rule to use when an entry has different DNs in the source and destination directories. The following values are allowed for the `dndif` argument:

- `ignore`: Ignore the conflict and take no action
- `usesrc`: Change the DN of the entry in the destination directory to that of the source directory
- `log2usesrc`: Same as `usesrc` except that the change is logged into an LDIF file, and not directly effected in the destination directory
- `usedest`: Change the DN of the entry in the source directory to that of the destination directory
- `log2usedest`: Same as `usedest` except that the change is logged into an LDIF file, and not directly effected in the source directory

The default value depends on the operation specified. [Table 4–7](#) shows the default values of the `mvatrdif` argument, corresponding to the operations specified.

**Table 4–7 Default Values for the `mvatrdif` Argument**

Operation	Default Value
compare	log2usesrc
reconcile	usesrc
merge	log2usesrc
merge_dryrun	usesrc
userdefinedcr	ignore

**`odefos=ignore | add | log2add | del | log2del | log`**

Optional. Specifies the conflict resolution rule to use when an object class definition exists only in the source directory. The following values are allowed for the `odefos` argument:

- `ignore`: Ignore the conflict and do not take any action
- `add`: Add the object class definition to the peer directory
- `log2add`: Same as `add` except that the changes are logged into an LDIF file and not directly effected in the directory.
- `del`: Delete the object class definition from the directory

- `log2del`: Same as `del` except that the changes are logged into an LDIF file and not directly effected in the directory
- `log`: Log the conflict in the report file and take no other action

The default value depends on the operation specified. [Table 4–8](#) shows the default values of the `odefos` argument, corresponding to the operations specified.

**Table 4–8 Default Values for the `odefos` Argument**

Operation	Default Value
<code>compare</code>	<code>log2add</code>
<code>reconcile</code>	<code>add</code>
<code>merge</code>	<code>add</code>
<code>merge_dryrun</code>	<code>log2add</code>
<code>userdefinedcr</code>	<code>ignore</code>

**`odefod=ignore | add | log2add | del | log2del | log`**

Optional. Specifies the conflict resolution rule to use when an object class definition exists only in the destination directory. The values allowed for the `odefod` argument are the same as the `odefos` argument.

The default value depends on the operation specified. [Table 4–9](#) shows the default values of the `odefod` argument, corresponding to the operations specified.

**Table 4–9 Default Values for the `odefod` Argument**

Operation	Default Value
<code>compare</code>	<code>log2del</code>
<code>reconcile</code>	<code>del</code>
<code>merge</code>	<code>add</code>
<code>merge_dryrun</code>	<code>log2add</code>
<code>userdefinedcr</code>	<code>ignore</code>

**`odefdif=ignore | usesrc | log2usesrc | usedest | log2usedest | merge | log2merge | log`**

Optional. Specifies the conflict resolution rule to use when an object class definition is different in the source and destination directories. The following values are allowed for the `odefdif` argument:

- `ignore`: Ignore the conflict and take no action
- `usesrc`: Replace the object class definition in the destination directory with the object class definition in the source directory
- `log2usesrc`: Same as `usesrc` except that the changes are logged in an LDIF file and not directly effected in the destination directory
- `usedest`: Replace the object class definition in the source directory with the object class definition in the destination directory
- `log2usedest`: Same as `usedest` except that the changes are logged in an LDIF file and not directly effected in the source directory
- `merge`: Merge the object class definitions. This involves adding optional and mandatory attributes available in one directory to the other directory

- `log2merge`: Same as `merge` except that the changes are logged into an LDIF file and not directly effected in the directory
- `log`: Log the conflicts in the report file and take no other action

The default value depends on the operation specified. [Table 4–10](#) shows the default values of the `odefdir` argument, corresponding to the operation specified.

**Table 4–10 Default Values for the `odefdir` Argument**

Operation	Default Value
<code>compare</code>	<code>log2usesrc</code>
<code>reconcile</code>	<code>usesrc</code>
<code>merge</code>	<code>merge</code>
<code>merge_dryrun</code>	<code>log2merge</code>
<code>userdefinedcr</code>	<code>ignore</code>

**`adefos=ignore | add | log2add | del | log2del | log`**

Optional. Specifies the conflict resolution rule to use when an attribute definition exists only in the source directory. The following values are allowed for the `adefos` argument:

- `ignore`: Ignore the conflict and do not take any action
- `add`: Add the attribute definition to the peer directory
- `log2add`: Same as `add` except that the changes are logged into an LDIF file and not directly effected in the directory.
- `del`: Delete the attribute definition from the directory
- `log2del`: Same as `del` except that the changes are logged into an LDIF file and not directly effected in the directory
- `log`: Log the conflict in the report file and take no other action

The default value depends on the operation specified. [Table 4–11](#) shows the default values of the `adefos` argument, corresponding to the operation specified.

**Table 4–11 Default Values for the `adefos` Argument**

Operation	Default Value
<code>compare</code>	<code>log2add</code>
<code>reconcile</code>	<code>add</code>
<code>merge</code>	<code>add</code>
<code>merge_dryrun</code>	<code>log2add</code>
<code>userdefinedcr</code>	<code>ignore</code>

**`adefod=ignore | add | log2add | del | log2del | log`**

Optional. Specifies the conflict resolution rule to use when an attribute definition exists only in the destination directory. The values allowed for the `adefod` argument are the same as the `adefos` argument.

The default value depends on the operation specified. [Table 4–12](#) shows the default values of the `adefod` argument, corresponding to the operation specified.

**Table 4–12 Default Values for the *adefod* Argument**

Operation	Default Value
compare	log2del
reconcile	del
merge	add
merge_dryrun	log2add
userdefinedcr	ignore

***adefdif=ignore | usesrc | log2usesrc | usedest | log2usedest | log***

Optional. Specifies the conflict resolution rule to use when an attribute definition is different in the source and destination directories. The following values are allowed for the *adefdif* argument:

- *ignore*: Ignore the conflict and take no action
- *usesrc*: Replace the attribute definition in the destination directory with the attribute definition in the source directory
- *log2usesrc*: Same as *usesrc* except that the changes are logged in an LDIF file and not directly effected in the destination directory
- *usedest*: Replace the attribute definition in the source directory with the attribute definition in the destination directory
- *log2usedest*: Same as *usedest* except that the changes are logged in an LDIF file and not directly effected in the source directory
- *log*: Log the conflicts in the report file and take no other action

The default value depends on the operation specified. [Table 4–13](#) shows the default values of the *adefdif* argument, corresponding to the operation specified.

**Table 4–13 Default Values for the *adefdif* Argument**

Operation	Default Value
compare	log2usesrc
reconcile	usesrc
merge	usesrc
merge_dryrun	log2usesrc
userdefinedcr	ignore

***paramfile=filename\_that\_contains\_the\_above\_parameters***

Optional. Specifies a parameter file to supply argument values. A parameter file can be used to supply arguments that are normally entered at the command line. The file should contain *argument=value* pairs either separated by whitespace characters or entered on separate lines. If an argument is contained in the parameter file and also supplied through the command line, then the command line value overrides the parameter file value for that argument.

***xmlParamFile=file\_containing\_parameters\_in\_XML\_format***

Optional. Specifies an XML parameter file to supply argument values. If an argument is contained in the parameter file and also supplied through the command line, then the command line value overrides the parameter file value for that argument.

## 4.2.3 Tasks and Examples for oidcmprec

This section provides examples for tasks that can be performed using the `oidcmprec` command. The following examples discuss various operations that can be performed with the `oidcmprec` tool:

- Section 4.2.3.1, "Comparing and Reconciling Individual Entries in Two Directories"
- Section 4.2.3.2, "Comparing and Reconciling Subtrees in Two Directories"
- Section 4.2.3.3, "Comparing and Reconciling Entire Directories"
- Section 4.2.3.4, "Performing User-Defined Compare and Reconcile Operations"
- Section 4.2.3.5, "Merging Two Directories"
- Section 4.2.3.6, "Including and Excluding Attributes"
- Section 4.2.3.7, "Using a Filter"
- Section 4.2.3.8, "Overriding Default Conflict Resolution Rules"
- Section 4.2.3.9, "Using a Parameter File"
- Section 4.2.3.10, "Using a Parameter File in XML Format"
- Section 4.2.3.11, "Generating Change Logs"
- Section 4.2.3.12, "Performing Directory Schema Operations"

### 4.2.3.1 Comparing and Reconciling Individual Entries in Two Directories

This example compares the DN, `"cn=Anne Smith,cn=users,dc=uk,dc=acme,dc=com"`, in the source and destination directories. The default conflict resolution rules for the `compare` operation are used. You are prompted for the source directory and destination directory passwords.

#### Example

```
oidcmprec base="cn=Anne Smith,cn=users,dc=uk,dc=acme,dc=com" \
operation=compare \
source=myhost1.acme.com:3060 \
destination=myhost2.acme.com:3060
```

```
Enter replication DN password of the source directory :
Enter replication DN password of the destination directory :
```

The following example compares the DN, `cn=Anne Smith,cn=users,dc=uk,dc=acme,dc=com`, in the source and destination directories. It resolves the conflicts that are detected. The default conflict resolution rules for the `reconcile` operation are used.

#### Example

```
oidcmprec base="cn=Anne Smith,cn=users,dc=uk,dc=acme,dc=com" \
operation=reconcile \
source=myhost1.acme.com:3060 \
destination=myhost2.acme.com:3060
```

### 4.2.3.2 Comparing and Reconciling Subtrees in Two Directories

This example compares the naming context, `dc=com`, in the two directories. The `scope` attribute has been set to `subtree`. This allows the entire directory information tree (DIT) under the base DN, `dc=com`, to be compared. The `threads` and `dnThreads` arguments



specify the number of worker threads and DN threads. The `cmpres` file is used to store the report for the operation.

### Example

```
oidcmprec base="dc=com" \
  operation=compare scope=subtree \
  source=myhost1.mycom.com:3060 \
  destination=myhost2.mycom.com:3060 \
  threads=5 dnthreads=2 filename=cmpres
```

The following example performs the reconcile operation on two subtrees namely, `dc=com` and `dc=org`. The `dns2exclude` argument is used to exclude the `c=us,dc=mycom,dc=com` and `c=uk,dc=myorg,dc=org` subtrees from the operation.

### Example

```
oidcmprec base="dc=com" "dc=org" \
  dns2exclude="c=us,dc=mycom,dc=com" "c=uk,dc=myorg,dc=org" \
  operation=reconcile scope=subtree \
  source=myhost1.mycom.com:3060 \
  destination=myhost2.mycom.com:3060 \
```

### 4.2.3.3 Comparing and Reconciling Entire Directories

The following example compares a directory residing on `host1` with another directory residing on `host2`. The `base` argument is set to `" "` and the `scope` argument is set to `subtree`.

### Example

```
oidcmprec operation=compare source=host1:3060 \
  destination=host2:3070 \ base=" " scope=subtree
```

The following example reconciles a directory residing on `myhost1` with another directory residing on `myhost2`. Entire directories are compared except the DN, `c=us,dc=mycom,dc=com`.

### Example

```
oidcmprec base=" " \
  dns2exclude="c=us,dc=mycom,dc=com" \
  operation=reconcile scope=subtree \
  source=myhost1.mycom.com:3060 \
  destination=myhost2.mycom.com:3060 \
  threads=5 dnthreads=2 file=cmpres
```

---

---

**Note:** When you compare entire directories, the following DNs and their subtrees are excluded:

- root DSE entry
- cn=auditlog
- cn=baseschema
- cn=catalogs
- cn=events
- cn=oracle internet directory
- cn=replication configuration
- cn=server configuration
- cn=subconfigsubentry
- cn=subregistrysubentry
- cn=subschemasubentry

You can include these entries by specifying them explicitly in the base argument.

---

---

#### 4.2.3.4 Performing User-Defined Compare and Reconcile Operations

This example makes use of user-defined values for the `-entos`, `-entod`, `-atros`, `-svatrdif`, `-mvatrdif`, and `-dndif` arguments. Conflict resolution arguments not specified on the command line, like `-atrod`, are set to ignore.

##### Example

```
oidcmprec operation=userdefinedcr scope=subtree \  
base="'dc=com' 'dc=org'" \  
source=myhost1.mycom.com:3060 \  
destination=myhost2.mycom.com:3060 \  
entos=add entod=ignore atros=add \  
svatrdif=usesrc mvatrdif=usesrc dndif=ignore \  
threads=5 dnthreads=2 file=myreconcile
```

#### 4.2.3.5 Merging Two Directories

This example synchronizes the `dc=com` subtree in two directories. The merge operation updates both the source and destination directories.

##### Example

```
oidcmprec operation=merge scope=subtree base="'dc=com'" \  
source=myhost1.mycom.com:3060 \  
destination=myhost2.mycom.com:3060 \  
file=merge
```

#### 4.2.3.6 Including and Excluding Attributes

The following example performs a compare operation. It uses the `exclattr` argument to exclude the `orclguid`, `category`, `userpassword`, and `authpassword` attributes. The example makes use of wildcard pattern matching to exclude the `authpassword` attribute subtypes.

**Example**

```
oidcmprec operation=compare scope=subtree base="'dc=com' 'dc=org'" \
source=myhost1.mycom.com:3060 \
destination=myhost2.mycom.com:3060 \
exclattr="userpassword authpassword authpassword;* orclguid category"
threads=5 dnthreads=2 file=compare
```

The following example makes use of the `inclattr` argument to include the `userpassword`, `cn`, `sn` `givenname`, and `mail` attributes.

**Example**

```
oidcmprec operation=compare scope=subtree base="'dc=com'" \
source=myhost1.mycom.com:3060 \
destination=myhost2.mycom.com:3060 \
inclattr="userpassword cn sn givenname mail"
file=cmp
```

The following example includes all attributes for the compare operation except `orclguid`, `creatorsname`, and `modifiersname` attributes.

**Example**

```
oidcmprec operation=compare scope=subtree base="'dc=com'" \
source=myhost1.mycom.com:3060 \
destination=myhost2.mycom.com:3060 \
inclattr="*" exclattr="orclguid creatorsname modifiersname"
file=compare
```

**4.2.3.7 Using a Filter**

The following example restricts the comparison to entries that match the filter (`cn=*`).

**Example**

```
oidcmprec source=stadd54:3060 destination=stadd54:3060 \
base="" scope=sub operation=compare file=test \
filter="'(cn=*)'"
```

**4.2.3.8 Overriding Default Conflict Resolution Rules**

This example performs a compare operation on two directories. It overrides the default conflict resolution rules used for the `dn dif` and `mvatrdif` arguments. The conflict resolution rule for these arguments is set to `ignore`.

**Example**

```
oidcmprec source=host1:3060 destination=host2:3070 \
base="" scope=subtree file=temp operation=compare \
dn dif=ignore mvatrdif=ignore
```

**4.2.3.9 Using a Parameter File**

This example performs a compare operation on two directories. It uses a parameter file, `comp_param` to specify command-line arguments. The `dnThreads` argument is specified both in the file and at the command line. The command-line value of `dnThreads` overrides the value specified in the parameter file.

**Example**

```
oidcmprec paramfile=comp_param dnthreads=3
```

The following displays the parameter file that is used:

```
#####
#Parameter file for compare and reconcile tool
#Creator   : John
#Date      : 21-Mar-2006
#File Name : comp_param
#####
operation=compare
source=stajj13:3060
destination=stajj13:3070
base="cn=oraclecontext"
base="c=uk,dc=mycom,dc=com"
base="c=us,dc=mycom,dc=com"
verbose=false
force=true
threads=6
dnthreads=2
exclattr="orclguid userpassword authpassword authpassword;*"
filename=cmp2006Feb01
```

#### 4.2.3.10 Using a Parameter File in XML Format

This example performs a compare operation on two directories.

##### Example

```
oidcmprec xmlParameterFile=param.xml
```

The following is an example of an XML parameter file:

```
<?xml version="1.0" standalone="yes" ?>
- <input>
  <operation>compare</operation>
- <source>
  <host>stadd54</host>
  <port>3060</port>
  <binddn>cn=orcladmin</binddn>
  <password>source-password</password>
  <isSSLPort>>false</isSSLPort>
</source>
- <destination>
  <host>stadd54</host>
  <port>3060</port>
  <binddn>cn=orcladmin</binddn>
  <password>destination-password</password>
  <isSSLPort>>true</isSSLPort>
</destination>
<base>
  <dn>dc=myhost,dc=example,dc=com</dn>
  <dn>cn=OracleSchemaVersion</dn>
</base>
<dns2exclude>
  <dn>cn=test instance,cn=oraclecontext</dn>
  <dn>ou=support,o=us</dn>
</dns2exclude>
<scope>subtree</scope>
<filter />
<threads>1</threads>
<dnthreads>1</dnthreads>
<inclattr />
```

```

<exclattr>
  <attribute>orclguid</attribute>
  <attribute>userpassword</attribute>
  <attribute>authpassword</attribute>
</exclattr>
<compareby>tool</compareby>
<filename>test</filename>
<genchglog>default</genchglog>
<force>true</force>
<verbose>false</verbose>
<contonerr>true</contonerr>
- <!--
  <entod>ignore</entod>
  <entos>ignore</entos>
  <atros>ignore</atros>
  <atrod>ignore</atrod>
  <svatrdif>ignore</svatrdif>
  <mvatrdif>ignore</mvatrdif>
  <dndif>ignore</dndif>
  <adefos>ignore</adefos>
  <adefod>ignore</adefod>
  <adefdif>ignore</adefdif>
  <odefos>ignore</odefos>
  <odefod>ignore</odefod>
  <odefdif>ignore</odefdif>

-->
</input>

```

Substitute the password for *password* in the example. Because the file contains a password, ensure that it is not readable by unauthorized users.

#### 4.2.3.11 Generating Change Logs

The following example uses the `genchglog` argument to ensure that change logs are generated for the operation. When `genchglog` is set to `true`, change logs are generated at both the source and destination directories.

##### Example

```

oidcmprec operation=merge scope=subtree base="'dc=com'" \
  source=myhost1.mycom.com:3060 \
  destination=myhost2.mycom.com:3060 \
  inclattr="*" exclattr="orclguid creatorsname modifiersname" \
  file=merge genchglog=true

```

#### 4.2.3.12 Performing Directory Schema Operations

The following example includes the schema for the selected operation by adding the `cn=subschemasubentry` DN to the base argument.

##### Example

```

oidcmprec operation=merge scope=subtree \
  base="'dc=com' 'cn=subschemasubentry'" \
  source=myhost1.mycom.com:3060 \
  destination=myhost2.mycom.com:3060 \
  inclattr="*" exclattr="orclguid creatorsname modifiersname" \
  file=merge genchglog=false

```

## 4.3 remtool

The Replication Environment Management Tool is used to manage Oracle Internet Directory replication configuration activities.

More specifically, the Replication Environment Management tool:

- Configures Oracle Database Advanced Replication-based multimaster replication.
- Scans the replication environment and verifies an Oracle Database Advanced Replication-based directory replication group (DRG).
- Rectifies any problems in an Oracle Database Advanced Replication-based DRG. If the tool cannot rectify a problem, it reports the point or points of failure, which you can then fix manually.
- Reports queue statistics, deferred transactions errors, and administrative request errors of an Oracle Database Advanced Replication-based DRG.
- Reconfigures the Oracle Database Advanced Replicationbased DRG.
- Configures LDAP-based replication.
- Reconfigures an LDAP-based directory replication group (DRG).
- Monitors replication progress in a DRG.

**See Also:** The section "Managing and Monitoring Replication by Using the Command Line" in *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*.

### 4.3.1 Syntax for remtool

```
remtool operation [connection_argument] [-v]
operation := { -addnode      | -asrsetup   | -chgpwd    | -delnode   |
               -asrcleanup  | -asrverify  | -asrrectify| -asrdisplay|
               -dispqstat   | -suspendasr| -resumeasr | -asr2ldap  |
               -dispasrerr  | -paddnode   | -pdelnode  | -pcleanup  |
               -pchgpwd    | -pdisplay   | -pchgmaster| [-multimaster]|
               -pchgwalpwd  | -pdispqstat| -pverify   | -presetpwd |
               -psuspendrepl -fromnode host1:port1 [-tonode host2:port2] |
               -presumerepl -fromnode host1:port1 [-tonode host2:port2]|
               -pthput [-interval time_in_seconds] [-file filename] }

connection_argument := { -bind supplier_hostname:ldap_port |
                        -connect repl_admin_name@net_service_name }
```

### 4.3.2 Terminology Used in remtool Argument Descriptions

In an Oracle Database Advanced Replication-based Directory Replication Group (DRG), one node must be identified as the Master Definition Site (MDS). This is the group master. All other nodes in the DRG are termed Remote Master Sites (RMS).

ODS.ASR\_CHG\_LOG and ODS.ODS\_CHG\_STAT are tables in Oracle Internet Directory's underlying database that store changelog information. The directory uses change logs to keep track of entries that are being replicated or that are being synchronized by the Oracle Directory Integration and Provisioning.

### 4.3.3 Arguments for remtool

#### operation

Required. The name of the operation to perform using `remtool`. See the appropriate operation documentation for command-specific syntax, arguments, and usage. The following operations are available:

- `-addnode` - Adds a new node to an Oracle Database Advanced Replication-based directory replication group (DRG). See [Section 4.3.5, "The remtool -addnode Operation"](#) for more information about this operation.
- `-asrsetup` - Creates a new directory replication group (DRG) by configuring Oracle Database Advanced Replication. See [Section 4.3.8, "The remtool -asrsetup Operation"](#) for more information about this operation.
- `-chgpwd` - Changes the replication administrator's database account password on all nodes of an Oracle Database Advanced Replication-based DRG. See [Section 4.3.11, "The remtool -chgpwd Operation"](#) for more information about this operation.
- `-delnode` - Deletes a node from an existing Oracle Database Advanced Replication-based DRG. See [Section 4.3.12, "The remtool -delnode Operation"](#) for more information about this operation.
- `-asrcleanup` - Cleans up the set up of an Oracle Database Advanced Replication-based DRG. See [Section 4.3.6, "The remtool -asrcleanup Operation"](#) for more information about this operation.
- `-asrverify` - Verifies the setup of Oracle Database Advanced Replication-based DRG, and reports any problems found. See [Section 4.3.9, "The remtool -asrverify Operation"](#) for more information about this operation.
- `-asrrectify` - Verifies the setup of Oracle Database Advanced Replication-based DRG, and corrects any problems found. See [Section 4.3.9, "The remtool -asrverify Operation"](#) for more information about this operation.
- `-asrdisplay` - Display all replica details in the replication group for an Oracle Database Advanced Replication-based setup.
- `-dispqstat` - Displays the queue statistics of all nodes in an Oracle Database Advanced Replication-based DRG. See [Section 4.3.14, "The remtool -dispqstat Operation"](#) for more information about this operation.
- `-suspendasr` - Suspends replication activity for an Oracle Database Advanced Replication-based DRG. See [Section 4.3.28, "The remtool -suspendasr Operation"](#) for more information about this operation.
- `-resumear` - Resumes replication activity for an Oracle Database Advanced Replication-based DRG. See [Section 4.3.27, "The remtool -resumear Operation"](#) for more information about this operation.
- `-asr2ldap` - Converts an existing Oracle Database Advanced Replication-based agreement to an LDAP multimaster agreement.
- `-dispasrerr` - Displays all deferred transaction errors and administrative request errors for an Oracle Database Advanced Replication-based DRG. See [Section 4.3.13, "The remtool -dispasrerr Operation"](#) for more information about this operation.
- `-paddnode` - Adds a partial replica to an LDAP-based DRG. See [Section 4.3.15, "The remtool -paddnode Operation"](#) for more information about this operation.

- `-pdelnod` - Deletes a partial replica from an LDAP-based DRG. See [Section 4.3.21, "The remtool -pdelnod Operation"](#) for more information about this operation.
- `-pcleanup` - Cleans up the partial replication setup of an LDAP-based DRG. See [Section 4.3.20, "The remtool -pcleanup Operation"](#) for more information about this operation.
- `-pchgpwd` - Changes the password of a replication DN for a replica in an LDAP-based DRG. See [Section 4.3.18, "The remtool -pchgpwd Operation"](#) for more information about this operation.
- `-pdisplay` - Displays all replica details in a partial replication group. See [Section 4.3.16, "The remtool -pdisplay Operation"](#) for more information about this operation.
- `pchgmaster` - Breaks agreement with an old LDAP-based supplier (master copy of the naming context) and reestablishes agreement with a new supplier. See [Section 4.3.17, "The remtool -pchgmaster Operation"](#) for more information about this operation.
- `-pchgwlpwd` - Changes the wallet password of a replication DN for a replica in an LDAP-based DRG. See [Section 4.3.19, "The remtool -pchgwlpwd Operation"](#) for more information about this operation.
- `-pdispqstat` - Displays the queue statistics for a directory replication group (DRG) that uses LDAP-based replication. See [Section 4.3.22, "The remtool -pdispqstat Operation"](#) for more information about this operation.
- `-pverify` - Verifies the replication configuration for a DRG node that uses LDAP-based replication. See [Section 4.3.26, "The remtool -pverify Operation"](#) for more information about this operation.
- `-presetpwd` - Resets the password of a replication DN for a replica in an LDAP-based DRG. See [Section 4.3.24, "The remtool -presetpwd Operation"](#) for more information about this operation.
- `-pilotreplica` - Begins or ends pilot mode for a replica. See [Section 4.3.23, "The remtool -pilotreplica Operation"](#) for more information about this operation.
- `-backupmetadata` - Adds the metadata of a pilot replica to a master replica or backs up the metadata of a pilot replica into a file. This operation must be executed at the pilot replica. See [Section 4.3.10, "The remtool -backupmetadata Operation"](#) for more information about this operation.
- `-psuspendrepl -fromnode host1:port1 [-tonode host2:port2]` - Only used during rolling upgrade. For more information, see the appendix "Performing a Rolling Upgrade" in *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*.
- `-presumerepl -fromnode host1:port1 [-tonode host2:port2]` - Only used during rolling upgrade. For more information, see the appendix "Performing a Rolling Upgrade" in *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*.
- `-pthput [-interval time_in_seconds] [-file filename]` - Enables you to monitor replication progress in a directory replication group. See [Section 4.3.25, "The remtool -pthput Operation"](#) for more information.

#### **connection\_argument**

The connection information to be supplied to `remtool`. The following connection details are available:



- `-bind` - Used with LDAP-based replication operations to specify the hostname and port of the supplier. See [Section 4.3.30, "The `-bind` Connection Argument"](#) for more information.
- `-connect` - Used with Oracle Database Advanced Replication-based replication options to specify the connection string for the master definition site (MDS) or the Remote Master Site (RMS). See [Section 4.3.31, "The `-connect` Connection Argument"](#) for more information.

**-v**

Optional. Runs the command in verbose mode. Shows detailed output for the command on the screen and also logs all operations in the `remtool.log` file created in `ORACLE_INSTANCE/OID/log`.

## 4.3.4 The `remtool -asr2ldap` Operation

If there is an existing Oracle Database Advanced Replication-based agreement between two or more nodes, you can convert this agreement to an LDAP multimaster agreement by using the `asr2ldap` operation.

### 4.3.4.1 Syntax for `remtool -asr2ldap`

```
remtool -asr2ldap
```

### 4.3.4.2 Arguments for `remtool -asr2ldap`

The tool prompts you for information, as shown in the example.

### 4.3.4.3 Tasks and Examples for `remtool -asr2ldap`

Using the `asr2ldap` operation, you can perform the following tasks:

- [Section 4.3.4.3.1, "Converting an Advanced Replication Agreement to an LDAP-Based Agreement"](#)

#### 4.3.4.3.1 Converting an Advanced Replication Agreement to an LDAP-Based Agreement

**Example:**

```
remtool -asr2ldap
```

The results are:

```
Enter replication administrator's name      : repadmin

Enter replication administrator's password :
Enter global name of MDS                   : inst1.regress.rdbms.dev.example.com
Directory Replication Group (DRG) details :

-----
Instance Host Name   Global Name           Version      ReplicaId   Site
Name                Type
-----
tst1    stacu14    INST1.REGRESS.RDBMS.DEV  OID 11.1.1.0.  stacu14_tst1  MDS
tst12   stacu14    INST2.REGRESS.RDBMS.DEV  OID 11.1.1.0.  stacu14_tst12 RMS
-----
Do you want to continue? [y/n] : y

-----
Migrating ASR agreement to LDAP MM agreement...
```

```

Enter "SYSTEM" user password for "INST2.REGRESS.RDBMS.DEV.EXAMPLE.COM" database at
"stacul4" host :
Enter "SYSTEM" user password for "INST1.REGRESS.RDBMS.DEV.example.com" database at
"stacul4" host :
-----
ASR setup has been cleaned
up.-----

```

## 4.3.5 The remtool -addnode Operation

The addnode operation adds a new node to an existing directory replication group (DRG). You must first create the DRG using [Section 4.3.5, "The remtool -addnode Operation."](#) The following usage rules apply to this operation:

- The node to be added must be empty.
- You must know the SYSTEM user password of the new node.
- Oracle Internet Directory processes on the master definition site (MDS) and other remote master sites (RMSs) must be down.
- After the addnode operation is complete, Oracle Internet Directory processes can be restarted.

### 4.3.5.1 Syntax for remtool -addnode

```
remtool -addnode [-connect repl_admin_name@net_service_name] [-v]
```

### 4.3.5.2 Arguments for remtool -addnode

The tool also prompts you for the database global name (as defined in the tnsnames.ora file) and SYSTEM password for each node to be added.

#### **-connect repl\_admin\_name@net\_service\_name**

For more information, see [Section 4.3.31, "The -connect Connection Argument."](#)

### 4.3.5.3 Tasks and Examples for remtool -addnode

Using the addnode operation you can perform the following tasks:

- [Section 4.3.5.3.1, "Adding a New Node to an Oracle Database Advanced Replication-based DRG"](#)

**4.3.5.3.1 Adding a New Node to an Oracle Database Advanced Replication-based DRG** In this example, MY\_HOST3.MY\_COMPANY.COM is added to a DRG consisting of MY\_HOST1.MY\_COMPANY.COM and MY\_HOST2.MY\_COMPANY.COM.

#### **Example:**

```
remtool -addnode -v -connect repadmin@MY_HOST1.MY_COMPANY.COM
```

The results are:

```

MY_HOST1.MY_COMPANY.COM is Master Definition Site (MDS). Connected to MDS.
MY_HOST2.MY_COMPANY.COM is Remote Master Site (RMS). Connected to RMS.
Directory Replication Group (DRG) details :

```

```

-----
Instance Host Name      Global Name              Version      Replicaid      Site
Name                                                            Type

```

```

-----
rid2      my_host      MY_HOST1.MY_COMPANY.COM  OID 10.1.2.0.0 my_host_rid1  MDS
rid2      my_host      MY_HOST2.MY_COMPANY.COM  OID 10.1.2.0.0 my_host_rid2  RMS
-----

```

Do you want to continue? [y/n] : y

-----  
WARNING:

Make sure that the replication administrator database account does not exist already in the new node to be added to the DRG. If the account exists, that account will be dropped and will be created newly.

-----  
Enter global name of new node to be added : MY\_HOST3.MY\_COMPANY.COM

Enter SYSTEM user password of new node to be added :  
-----

Adding a new node...

```

MY_HOST3.MY_COMPANY.COM : Verifying uniqueness of replication agreement entry...
MY_HOST3.MY_COMPANY.COM : Dropping replication administrator repadmin...
MY_HOST3.MY_COMPANY.COM : Creating replication administrator repadmin...
MY_HOST3.MY_COMPANY.COM : Granting privileges or roles required for replication
administrator to repadmin...
MY_HOST3.MY_COMPANY.COM : Granting privileges or roles required for replication
administrator to repadmin...
MY_HOST3.MY_COMPANY.COM : Granting privileges or roles required for replication
administrator to repadmin...
MY_HOST3.MY_COMPANY.COM : Dropping replication group LDAP_REP...
MY_HOST3.MY_COMPANY.COM : Creating purge job...
MY_HOST3.MY_COMPANY.COM : Dropping database link made to
MY_HOST1.MY_COMPANY.COM...
MY_HOST3.MY_COMPANY.COM : Dropping database link made to
MY_HOST1.MY_COMPANY.COM...
MY_HOST3.MY_COMPANY.COM : Creating database link to MY_HOST1.MY_COMPANY.COM...
MY_HOST3.MY_COMPANY.COM : Scheduling push job to MY_HOST1.MY_COMPANY.COM...
MY_HOST3.MY_COMPANY.COM : Dropping database link made to
MY_HOST2.MY_COMPANY.COM...
MY_HOST3.MY_COMPANY.COM : Dropping database link made to
MY_HOST2.MY_COMPANY.COM...
MY_HOST3.MY_COMPANY.COM : Creating database link to MY_HOST2.MY_COMPANY.COM...
MY_HOST3.MY_COMPANY.COM : Scheduling push job to MY_HOST2.MY_COMPANY.COM...
MY_HOST1.MY_COMPANY.COM : Dropping database link made to
MY_HOST3.MY_COMPANY.COM...
MY_HOST1.MY_COMPANY.COM : Dropping database link made to
MY_HOST3.MY_COMPANY.COM...
MY_HOST1.MY_COMPANY.COM : Creating database link to MY_HOST3.MY_COMPANY.COM...
MY_HOST1.MY_COMPANY.COM : Scheduling push job to MY_HOST3.MY_COMPANY.COM...
MY_HOST2.MY_COMPANY.COM : Dropping database link made to
MY_HOST3.MY_COMPANY.COM...
MY_HOST2.MY_COMPANY.COM : Dropping database link made to
MY_HOST3.MY_COMPANY.COM...
MY_HOST2.MY_COMPANY.COM : Creating database link to MY_HOST3.MY_COMPANY.COM...
MY_HOST2.MY_COMPANY.COM : Scheduling push job to MY_HOST3.MY_COMPANY.COM...
MY_HOST1.MY_COMPANY.COM : Quiescing replication activity...
MY_HOST1.MY_COMPANY.COM : Adding replication site MY_HOST3.MY_COMPANY.COM to
replication group LDAP_REP...
MY_HOST1.MY_COMPANY.COM : Executing deferred administrative requests...
MY_HOST3.MY_COMPANY.COM : Executing deferred administrative requests...
MY_HOST1.MY_COMPANY.COM : Executing deferred administrative requests...

```

```

MY_HOST1.MY_COMPANY.COM : Executing deferred administrative requests...
MY_HOST3.MY_COMPANY.COM : Executing deferred administrative requests...
MY_HOST1.MY_COMPANY.COM : Resuming replication activity...
MY_HOST1.MY_COMPANY.COM : Verifying uniqueness of replication agreement entry...
MY_HOST2.MY_COMPANY.COM : Verifying uniqueness of replication agreement entry...
MY_HOST3.MY_COMPANY.COM : Verifying uniqueness of replication agreement entry...
MY_HOST1.MY_COMPANY.COM : Verifying replication agreement entry...
MY_HOST1.MY_COMPANY.COM : Inserting replication agreement entry my_host_rid3...
CORRECTED:
MY_HOST1.MY_COMPANY.COM : "my_host_rid3" hostname has been added to replication
agreement entry.
MY_HOST2.MY_COMPANY.COM : Verifying replication agreement entry...
MY_HOST2.MY_COMPANY.COM : Inserting replication agreement entry my_host_rid3...
CORRECTED:
MY_HOST2.MY_COMPANY.COM : "my_host_rid3" hostname has been added to replication
agreement entry.
MY_HOST3.MY_COMPANY.COM : Verifying replication agreement entry...
MY_HOST3.MY_COMPANY.COM : Inserting replication agreement entry my_host_rid...
CORRECTED:
MY_HOST3.MY_COMPANY.COM : "my_host_rid" hostname has been added to replication
agreement entry.
MY_HOST3.MY_COMPANY.COM : Inserting replication agreement entry my_host_rid2...
CORRECTED:
MY_HOST3.MY_COMPANY.COM : "my_host_rid2" hostname has been added to replication
agreement entry.
MY_HOST3.MY_COMPANY.COM : Inserting replication agreement entry my_host_rid3...
CORRECTED:
MY_HOST3.MY_COMPANY.COM : "my_host_rid3" hostname has been added to replication
agreement entry.
MY_HOST1.MY_COMPANY.COM : Verifying initialization parameter...
MY_HOST2.MY_COMPANY.COM : Verifying initialization parameter...
MY_HOST3.MY_COMPANY.COM : Verifying initialization parameter...

```

```

-----
Node MY_HOST3.MY_COMPANY.COM has been added to this DRG.
-----

```

```

Directory Replication Group (DRG) details :

```

```

-----
Instance Host Name      Global Name              Version      ReplicaId      Site
Name                                                            Type
-----
rid1    my_host                 MY_HOST1.MY_COMPANY.COM  OID 10.1.2.0.0  my_host_rid1  MDS
rid2    my_host                 MY_HOST2.MY_COMPANY.COM  OID 10.1.2.0.0  my_host_rid2  RMS
rid3    my_host                 MY_HOST3.MY_COMPANY.COM  OID 10.1.2.0.0  my_host_rid3  RMS
-----

```

## 4.3.6 The remtool -asrcleanup Operation

The `asrcleanup` operation cleans up an existing Oracle Database Advanced Replication-based setup. You must know the system password of all nodes taking part in the directory replication group (DRG) to run this operation.

### 4.3.6.1 Syntax for remtool -asrcleanup

```
remtool -asrcleanup [-connect repl_admin_name@net_service_name] [-v]
```

### 4.3.6.2 Arguments for remtool -asrcleanup

The tool prompts you for the SYSTEM user password for each MDS and RMS node in the DRG

**-connect repl\_admin\_name@net\_service\_name**

For more information, see [Section 4.3.31, "The -connect Connection Argument."](#)

**4.3.6.3 Tasks and Examples for remtool -asrcleanup**

Using the asrcleanup operation you can perform the following tasks:

- [Section 4.3.6.3.1, "Cleaning Up an Oracle Database Advanced Replication-based DRG Setup"](#)

**4.3.6.3.1 Cleaning Up an Oracle Database Advanced Replication-based DRG Setup** In this example, setup is cleaned up for a DRG consisting of MY\_HOST1.MY\_COMPANY.COM and MY\_HOST2.MY\_COMPANY.COM. The tool prompts you to enter the system password for each site.

**Example:**

```
remtool -asrcleanup -v
```

The results are:

```
Enter replication administrator's name      : repadmin

Enter replication administrator's password :
Enter global name of MDS                   : my_host1.my_company.com

MY_HOST1.MY_COMPANY.COM is Master Definition Site (MDS). Connected to MDS.
MY_HOST2.MY_COMPANY.COM is Remote Master Site (RMS). Connected to RMS.
Directory Replication Group (DRG) details :

-----
Instance Host Name      Global Name              Version      ReplicaId      Site
Name                                                            Type
-----
rid1      my_host      MY_HOST1.MY_COMPANY.COM 10.1.2.0.0  my_host_rid1  MDS
rid2      my_host      MY_HOST2.MY_COMPANY.COM 10.1.2.0.0  my_host_rid2  RMS
-----

Do you want to continue? [y/n] : y

-----
Cleaning up...

MY_HOST1.MY_COMPANY.COM : Dropping replication site MY_HOST2.MY_COMPANY.COM from
replication group LDAP_REP...
MY_HOST2.MY_COMPANY.COM : Dropping replication group LDAP_REP...
MY_HOST2.MY_COMPANY.COM : Unscheduling push job to MY_HOST1.MY_COMPANY.COM...
MY_HOST2.MY_COMPANY.COM : Dropping database link made to
MY_HOST1.MY_COMPANY.COM...
MY_HOST2.MY_COMPANY.COM : Dropping database link made to
MY_HOST1.MY_COMPANY.COM...
Enter "SYSTEM" user password for "MY_HOST2.MY_COMPANY.COM" database at "my_host"
host :
MY_HOST2.MY_COMPANY.COM : Dropping replication administrator repadmin...
MY_HOST1.MY_COMPANY.COM : Dropping replication group LDAP_REP...
MY_HOST1.MY_COMPANY.COM : Unscheduling push job to MY_HOST2.MY_COMPANY.COM...
MY_HOST1.MY_COMPANY.COM : Dropping database link made to MY_HOST2.MY_COMPANY.COM...
MY_HOST1.MY_COMPANY.COM : Dropping database link made to
MY_HOST2.MY_COMPANY.COM...
Enter "SYSTEM" user password for "MY_HOST1.MY_COMPANY.COM" database at "my_host"
host :
```

```
MY_HOST1.MY_COMPANY.COM : Dropping replication administrator repadmin...
```

```
-----  
ASR setup has been cleaned up.  
-----
```

## 4.3.7 The remtool -asrrectify Operation

The `asrrectify` operation is used for detecting and rectifying problems in an Oracle Database Advanced Replication-based DRG setup. It reports on errors and corrects them. Oracle Corporation recommends that, before running this operation, you stop Oracle Internet Directory servers. To use the `asrrectify` operation, all nodes in the DRG must be up and running. The operation fails if any of the nodes are not running. If necessary, the `asrrectify` operation prompts for the SYSTEM user password.

### 4.3.7.1 Syntax for remtool -asrrectify

```
remtool -asrrectify [-connect repl_admin_name@net_service_name] [-v]
```

### 4.3.7.2 Arguments for remtool -asrrectify

The tool may also prompt you for the SYSTEM user password for each MDS and RMS node in the DRG.

#### **-connect repl\_admin\_name@net\_service\_name**

For more information, see [Section 4.3.31, "The -connect Connection Argument."](#)

### 4.3.7.3 Tasks and Examples for remtool -asrrectify

Using the `asrrectify` operation you can perform the following tasks:

- [Section 4.3.7.3.1, "Detecting and Correcting Errors in an Advanced Replication-Based DRG Setup"](#)

**4.3.7.3.1 Detecting and Correcting Errors in an Advanced Replication-Based DRG Setup** In this example, setup errors are deducted and rectified in a DRG consisting of `MY_HOST1.MY_COMPANY.COM` and `MY_HOST2.MY_COMPANY.COM`. The tool detects that a user has changed global name of `MY_HOST2.MY_COMPANY.COM` to `NEWNAME.MY_COMPANY.COM` after setting up Advanced Replication. It rectifies this error first before continuing with other checks.

#### **Example:**

```
remtool -asrrectify -v -conn repadmin@my_host1.my_company.com
```

The results are:

```
MY_HOST1.MY_COMPANY.COM is Master Definition Site (MDS). Connected to MDS.  
Enter "SYSTEM" user password for "MY_HOST2.MY_COMPANY.COM" database at "my_host"  
host :  
NEWNAME.MY_COMPANY.COM : Renaming global name to MY_HOST2.MY_COMPANY.COM (instance  
name : rid2, hostname : my_host)  
CORRECTED:  
MY_HOST2.MY_COMPANY.COM : Global name of database "rid2" at host "my_host" has  
been changed to MY_HOST2.MY_COMPANY.COM.  
MY_HOST2.MY_COMPANY.COM is Remote Master Site (RMS). Connected to RMS.  
CORRECTED:  
MY_HOST2.MY_COMPANY.COM : Global name of database "rid2" at host "my_host" has  
been changed to MY_HOST2.MY_COMPANY.COM.  
Directory Replication Group (DRG) details :
```

```

-----
Instance Host Name      Global Name              Version      ReplicaId      Site
Name                                                    Type
-----
rid1      my_host      MY_HOST1.MY_COMPANY.COM 10.1.2.0.0  my_host_rid1  MDS
rid2      my_host      MY_HOST2.MY_COMPANY.COM 10.1.2.0.0  my_host_rid2  RMS
-----
Do you want to continue? [y/n] : y

-----
Rectifying ASR setup...

MY_HOST1.MY_COMPANY.COM : Verifying initialization parameter...
MY_HOST2.MY_COMPANY.COM : Verifying initialization parameter...
MY_HOST1.MY_COMPANY.COM : Verifying replication administrator roles...
MY_HOST2.MY_COMPANY.COM : Verifying replication administrator roles...
MY_HOST1.MY_COMPANY.COM : Verifying database links...
MY_HOST2.MY_COMPANY.COM : Verifying database links...
MY_HOST1.MY_COMPANY.COM : Verifying purge job...
MY_HOST2.MY_COMPANY.COM : Verifying purge job...
MY_HOST1.MY_COMPANY.COM : Verifying scheduled links...
MY_HOST2.MY_COMPANY.COM : Verifying scheduled links...
MY_HOST1.MY_COMPANY.COM : Verifying availability of replication objects...
MY_HOST2.MY_COMPANY.COM : Verifying availability of replication objects...
MY_HOST1.MY_COMPANY.COM : Verifying replication group...
MY_HOST1.MY_COMPANY.COM : Resuming replication activity...
MY_HOST2.MY_COMPANY.COM : Verifying replication group...
MY_HOST1.MY_COMPANY.COM : Resuming replication activity...
MY_HOST1.MY_COMPANY.COM : Verifying uniqueness of replication agreement entry...
MY_HOST2.MY_COMPANY.COM : Verifying uniqueness of replication agreement entry...
MY_HOST1.MY_COMPANY.COM : Verifying replication agreement entry...
MY_HOST2.MY_COMPANY.COM : Verifying replication agreement entry...

-----
DB Name          Init   Repl   DB    Purge  Sch.  Repl  Repl
                  Param Admin Links Job    Links Group Agrmt
                  Role
-----
MY_HOST1.MY_COMPANY. Chkd  Chkd  Chkd  Chkd  Chkd  Chkd  Chkd
MY_HOST2.MY_COMPANY. Chkd  Chkd  Chkd  Chkd  Chkd  Chkd  Chkd
-----
Legends :
  Chkd - Checked. No errors.
  Crtd - ASR setup errors were found and corrected.
  Err  - Error occurred while doing ASR setup verification.
  NCrtd - ASR setup has errors, but not corrected.
-----

```

### 4.3.8 The remtool -asrsetup Operation

The asrsetup operation is used to create a new Oracle Database Advanced Replication-based directory replication group (DRG). A DRG consists of a master definition site (MDS) and one or more remote master sites (RMS).

Before you begin, stop all Oracle Internet Directory server processes on the MDS and RMS sites. After the setup operation is completed, you can restart all Oracle Internet Directory processes and replication server processes.

### 4.3.8.1 Syntax for remtool -asrsetup

```
remtool -asrsetup [-v]
```

### 4.3.8.2 Arguments for remtool -asrsetup

Only the optional `-v` argument is specified on the command-line. The tool prompts you for the following information.

- The database global name of the MDS (as defined in the `tnsnames.ora` file).
- A replication administrator password for the MDS
- The SYSTEM password for the MDS
- The database global for each RMS (as defined in the `tnsnames.ora` file).
- The SYSTEM password for each RMS

### 4.3.8.3 Tasks and Examples for remtool -asrsetup

Using the `asrsetup` operation you can perform the following tasks:

- [Section 4.3.8.3.1, "Creating an Oracle Database Advanced Replication-based DRG"](#)

**4.3.8.3.1 Creating an Oracle Database Advanced Replication-based DRG** In this example, a DRG is created consisting of `MY_HOST1.MY_COMPANY.COM` and `MY_HOST2.MY_COMPANY.COM`.

#### Example:

```
remtool -asrsetup -v
```

The results are as follows:

```
-----
ASR Setup for OID Replication
WARNING:
Make sure that the replication administrator that you
enter below does not exist already in any of the nodes
that will be part of the DRG to be created now. If the
user exists, that user will be dropped and will be
created newly.
-----
Enter replication administrator's name      : repadmin

Enter replication administrator's password  :
Reenter replication administrator's password :
Enter Master Definition Site (MDS) details  :
Enter global name of MDS                   : MY_HOST1.MY_COMPANY.COM

Enter SYSTEM user password of MDS          :
Enter Remote Master Site (RMS) details     :
Enter global name of RMS # 1                : MY_HOST2.MY_COMPANY.COM

Enter SYSTEM user password of MDS          :
Are there more Remote Master Sites in the group? [y/n/q] : n

Verify the details you had entered.
-----
Replication administrator's name      : repadmin
Master Definition Site                 : MY_HOST1.MY_COMPANY.COM
Remote Master Site # 1                  : MY_HOST2.MY_COMPANY.COM
Are these details correct? [y/n/q] : y
```



-----  
ASR setup in progress...

MY\_HOST1.MY\_COMPANY.COM : Verifying uniqueness of replication agreement entry...  
MY\_HOST1.MY\_COMPANY.COM : Dropping replication administrator repadmin...  
MY\_HOST1.MY\_COMPANY.COM : Creating replication administrator repadmin...  
MY\_HOST1.MY\_COMPANY.COM : Granting privileges or roles required for replication administrator to repadmin...  
MY\_HOST1.MY\_COMPANY.COM : Granting privileges or roles required for replication administrator to repadmin...  
MY\_HOST1.MY\_COMPANY.COM : Granting privileges or roles required for replication administrator to repadmin...  
MY\_HOST1.MY\_COMPANY.COM : Creating purge job...  
MY\_HOST1.MY\_COMPANY.COM : Dropping database link made to  
MY\_HOST2.MY\_COMPANY.COM...  
MY\_HOST1.MY\_COMPANY.COM : Dropping database link made to  
MY\_HOST2.MY\_COMPANY.COM...  
MY\_HOST1.MY\_COMPANY.COM : Creating database link to MY\_HOST2.MY\_COMPANY.COM...  
MY\_HOST1.MY\_COMPANY.COM : Scheduling push job to MY\_HOST2.MY\_COMPANY.COM...  
MY\_HOST2.MY\_COMPANY.COM : Verifying uniqueness of replication agreement entry...  
MY\_HOST2.MY\_COMPANY.COM : Dropping replication administrator repadmin...  
MY\_HOST2.MY\_COMPANY.COM : Creating replication administrator repadmin...  
MY\_HOST2.MY\_COMPANY.COM : Granting privileges or roles required for replication administrator to repadmin...  
MY\_HOST2.MY\_COMPANY.COM : Granting privileges or roles required for replication administrator to repadmin...  
MY\_HOST2.MY\_COMPANY.COM : Granting privileges or roles required for replication administrator to repadmin...  
MY\_HOST2.MY\_COMPANY.COM : Creating purge job...  
MY\_HOST2.MY\_COMPANY.COM : Dropping database link made to  
MY\_HOST1.MY\_COMPANY.COM...  
MY\_HOST2.MY\_COMPANY.COM : Dropping database link made to  
MY\_HOST1.MY\_COMPANY.COM...  
MY\_HOST2.MY\_COMPANY.COM : Creating database link to MY\_HOST1.MY\_COMPANY.COM...  
MY\_HOST2.MY\_COMPANY.COM : Scheduling push job to MY\_HOST1.MY\_COMPANY.COM...  
MY\_HOST1.MY\_COMPANY.COM : Dropping replication group LDAP\_REP...  
MY\_HOST1.MY\_COMPANY.COM : Creating replication group LDAP\_REP...  
MY\_HOST1.MY\_COMPANY.COM : Adding object TABLE ODS.ASR\_CHG\_LOG to replication group LDAP\_REP...  
MY\_HOST1.MY\_COMPANY.COM : Generating replication support for TABLE ODS.ASR\_CHG\_LOG...  
MY\_HOST1.MY\_COMPANY.COM : Adding object TABLE ODS.ODS\_CHG\_STAT to replication group LDAP\_REP...  
MY\_HOST1.MY\_COMPANY.COM : Generating replication support for TABLE ODS.ODS\_CHG\_STAT...  
MY\_HOST2.MY\_COMPANY.COM : Dropping replication group LDAP\_REP...  
MY\_HOST1.MY\_COMPANY.COM : Adding replication site MY\_HOST2.MY\_COMPANY.COM to replication group LDAP\_REP...  
MY\_HOST1.MY\_COMPANY.COM : Executing deferred administrative requests...  
MY\_HOST2.MY\_COMPANY.COM : Executing deferred administrative requests...  
MY\_HOST1.MY\_COMPANY.COM : Executing deferred administrative requests...  
MY\_HOST1.MY\_COMPANY.COM : Executing deferred administrative requests...  
MY\_HOST2.MY\_COMPANY.COM : Executing deferred administrative requests...  
MY\_HOST1.MY\_COMPANY.COM : Executing deferred administrative requests...  
MY\_HOST2.MY\_COMPANY.COM : Executing deferred administrative requests...  
MY\_HOST1.MY\_COMPANY.COM : Executing deferred administrative requests...  
MY\_HOST2.MY\_COMPANY.COM : Executing deferred administrative requests...  
MY\_HOST1.MY\_COMPANY.COM : Verifying initialization parameter...  
MY\_HOST2.MY\_COMPANY.COM : Verifying initialization parameter...

```

MY_HOST1.MY_COMPANY.COM : Verifying uniqueness of replication agreement entry...
MY_HOST2.MY_COMPANY.COM : Verifying uniqueness of replication agreement entry...
MY_HOST1.MY_COMPANY.COM : Verifying replication agreement entry...
MY_HOST1.MY_COMPANY.COM : Inserting replication agreement entry my_host...
CORRECTED:
MY_HOST1.MY_COMPANY.COM : "my_host_rid" hostname has been added to replication
agreement entry.
MY_HOST1.MY_COMPANY.COM : Inserting replication agreement entry my_host_rid2...
CORRECTED:
MY_HOST1.MY_COMPANY.COM : "my_host_rid2" hostname has been added to replication
agreement entry.
MY_HOST2.MY_COMPANY.COM : Verifying replication agreement entry...
MY_HOST2.MY_COMPANY.COM : Inserting replication agreement entry my_host_rid...
CORRECTED:
MY_HOST2.MY_COMPANY.COM : "my_host_rid1" hostname has been added to replication
agreement entry.
MY_HOST2.MY_COMPANY.COM : Inserting replication agreement entry my_host_rid2...
CORRECTED:
MY_HOST2.MY_COMPANY.COM : "my_host_rid2" hostname has been added to replication
agreement entry.
MY_HOST1.MY_COMPANY.COM : Resuming replication activity...
-----
ASR setup has been configured successfully.
-----
Directory Replication Group (DRG) details :
-----

```

Instance Name	Host Name	Global Name	Version	Replicaid	Site Type
rid1	my_host	MY_HOST1.MY_COMPANY.COM	OID 10.1.2.0.0	my_host_rid1	MDS
rid2	my_host	MY_HOST2.MY_COMPANY.COM	OID 10.1.2.0.0	my_host_rid2	RMS

### 4.3.9 The remtool -asrverify Operation

This `asrverify` operation detects and reports on problems found in an Oracle Database Advanced Replication-based directory replication group (DRG). This operation reports errors, but does not correct them. To run this operation, all nodes in the DRG must be up and running. You do not have to stop your Oracle Internet Directory server processes to run this operation.

The `asrverify` operation fails or report errors for the following situations. You can use the `asrrectify` operation to correct these errors. See [Section 4.3.9, "The remtool -asrverify Operation"](#) for more information about that operation.

- If, by mistake, the replication administrator account is dropped in any of the nodes, the `asrverify` operation fails. Use `asrrectify` to re-create the replication administrator account and add it back to the DRG.
- If, by mistake, the password for the replication administrator account has changed on any of the nodes in the DRG, the `asrverify` operation fails. Use `remtool asrrectify` to change the replication administrator account and add it back to the DRG.
- If the global database name of any node has changed after Advanced Replication setup, `asrverify` reports an error and does not proceed further. Use `asrrectify` to revert back to the previous global name and rectify other issues.

### 4.3.9.1 Syntax for remtool -asrverify

```
remtool -asrverify [-connect repl_admin_name@net_service_name] [-v]
```

### 4.3.9.2 Arguments for remtool -asrverify

#### -connect repl\_admin\_name@net\_service\_name

For more information, see [Section 4.3.31, "The -connect Connection Argument."](#)

### 4.3.9.3 Tasks and Examples for remtool -asrverify

Using the asrverify operation you can perform the following tasks:

- [Section 4.3.9.3.1, "Detecting Errors in an Oracle Database Advanced Replication-Based DRG Setup"](#)

#### 4.3.9.3.1 Detecting Errors in an Oracle Database Advanced Replication-Based DRG Setup

In this example, errors are found in a DRG consisting of two nodes.

##### Example:

```
remtool -asrverify -v -conn repadmin@my_host1.my_company.com
```

The results are:

```
MY_HOST1.MY_COMPANY.COM is Master Definition Site (MDS). Connected to MDS.
MY_HOST2.MY_COMPANY.COM is Remote Master Site (RMS). Connected to RMS.
Directory Replication Group (DRG) details :
```

```
-----
Instance Host Name      Global Name              Version      ReplicaId      Site
Name                                                            Type
-----
rid1    my_host    MY_HOST1.MY_COMPANY.COM  OID 10.1.2.0.0  my_host_rid1   MDS
rid2    my_host    MY_HOST2.MY_COMPANY.COM  OID 10.1.2.0.0  my_host_rid2   RMS
-----
```

```
Verifying ASR setup...
```

```
MY_HOST1.MY_COMPANY.COM : Verifying initialization parameter...
MY_HOST2.MY_COMPANY.COM : Verifying initialization parameter...
MY_HOST1.MY_COMPANY.COM : Verifying replication administrator roles...
MY_HOST2.MY_COMPANY.COM : Verifying replication administrator roles...
MY_HOST1.MY_COMPANY.COM : Verifying database links...
MY_HOST2.MY_COMPANY.COM : Verifying database links...
MY_HOST1.MY_COMPANY.COM : Verifying purge job...
MY_HOST2.MY_COMPANY.COM : Verifying purge job...
MY_HOST1.MY_COMPANY.COM : Verifying scheduled links...
MY_HOST2.MY_COMPANY.COM : Verifying scheduled links...
MY_HOST1.MY_COMPANY.COM : Verifying availability of replication objects...
MY_HOST2.MY_COMPANY.COM : Verifying availability of replication objects...
MY_HOST1.MY_COMPANY.COM : Verifying replication group...
ASR SETUP ERROR/WARNING:
MY_HOST1.MY_COMPANY.COM : Replication support is not available for TABLE
ODS.ASR_CHG_LOG.
ASR SETUP ERROR/WARNING:
MY_HOST1.MY_COMPANY.COM : Replication support is not available for TABLE
ODS.ODS_CHG_STAT.
MY_HOST2.MY_COMPANY.COM : Verifying replication group...
ASR SETUP ERROR/WARNING:
MY_HOST2.MY_COMPANY.COM : Replication support is not available for TABLE
```

```

ODS.ASR_CHG_LOG.
ASR SETUP ERROR/WARNING:
MY_HOST2.MY_COMPANY.COM : Replication support is not available for TABLE
ODS.ODS_CHG_STAT.
MY_HOST1.MY_COMPANY.COM : Verifying uniqueness of replication agreement entry...
MY_HOST2.MY_COMPANY.COM : Verifying uniqueness of replication agreement entry...
MY_HOST1.MY_COMPANY.COM : Verifying replication agreement entry...
MY_HOST2.MY_COMPANY.COM : Verifying replication agreement entry...

```

DB Name	Init Param	Repl Admin Role	DB Links	Purge Job	Sch. Links	Repl Group	Repl Agrmt Entry
MY_HOST1.MY_COMPANY.	Chkd	Chkd	Chkd	Chkd	Chkd	NCrtd	Chkd
MY_HOST2.MY_COMPANY.	Chkd	Chkd	Chkd	Chkd	Chkd	NCrtd	Chkd

Legends :

```

Chkd - Checked. No errors.
Crtd - ASR setup errors were found and corrected.
Err - Error occurred while doing ASR setup verification.
NCrtd - ASR setup has errors, but not corrected.

```

Summary of findings:

```

ASR SETUP ERROR/WARNING:
MY_HOST1.MY_COMPANY.COM : Replication support is not available for TABLE
ODS.ASR_CHG_LOG.

```

```

ASR SETUP ERROR/WARNING:
MY_HOST1.MY_COMPANY.COM : Replication support is not available for TABLE
ODS.ODS_CHG_STAT.

```

```

ASR SETUP ERROR/WARNING:
MY_HOST2.MY_COMPANY.COM : Replication support is not available for TABLE
ODS.ASR_CHG_LOG.

```

```

ASR SETUP ERROR/WARNING:
MY_HOST2.MY_COMPANY.COM : Replication support is not available for TABLE
ODS.ODS_CHG_STAT.

```

## 4.3.10 The remtool -backupmetadata Operation

The backupmetadata operation adds the metadata of a pilot replica to the master replica, or backs up the metadata of a pilot replica into a file.

---

**Note:** The -backupmetadata option does not work if anonymous bind is disabled at the pilot replica or master replica.

---

### 4.3.10.1 Syntax for remtool -backupmetadata

```

remtool -backupmetadata -replica pilot_hostname:port {-master master_hostname:port
| -bkup file_name} [-nwurl <file:wallet_location>] [-wurl <file:wallet_location>]

```

### 4.3.10.2 Arguments for remtool -backupmetadata

#### **-replica pilot\_hostname:port**

Required. The connection string for the pilot replica. You are prompted for the password for the replication DN of the pilot replica. The string is comprised of the following elements:

- The host name where the pilot replica's LDAP server is running.
- The pilot replica's LDAP listening port, for example 3060.

#### **-master master\_hostname:port**

Either `-master` or `-bkup` argument is required. (You can provide both arguments.) The connection string for the master replica. You are prompted for the password for the replication DN of the master replica. The string is comprised of the following elements:

- The host name where the master replica's LDAP server is running.
- The master replica's LDAP listening port, for example 3060.

#### **-bkup file\_name**

Either `-master` or `-bkup` argument is required. (You can provide both arguments.) The full path and file name of the LDIF output file. The metadata entries are written to this file in LDIF format.

#### **-nwurl file:wallet\_location**

The wallet location for SSL connection to the pilot replica (one-way or two-way).

#### **-wurl file:wallet\_location**

The wallet location for SSL connection to the master replica (one-way or two-way).

### 4.3.10.3 Tasks and Examples for remtool -backupmetadata

Using the `backupmetadata` operation you can perform the following tasks:

- [Section 4.3.10.3.1, "Adding the Metadata of a Pilot Replica to a Master Replica"](#)
- [Section 4.3.10.3.2, "Backing Up the Metadata of a Pilot Replica to an LDIF File"](#)

**4.3.10.3.1 Adding the Metadata of a Pilot Replica to a Master Replica** This example shows how to add the metadata entries from a pilot replica to a master replica.

#### **Example:**

```
remtool -backupmetadata -replica mypilot.company.com:3060 \
  -master mymaster.company.com:3060 -bkup /myfiles/backup.ldif
```

In this example, a backup file was specified with `-bkup`. The command output is:

```
Backup of metadata will be stored in /myfiles/backup.ldifMetadata copied
successfully.
```

#### **Example:**

```
remtool -backupmetadata -replica mypilot.company.com:3060 \
  -master mymaster.company.com:3060
```

In this example, no backup file was specified, so remtool uses the default location. The command output is:

```
Backup of metadata will be stored in
ORACLE_INSTANCE/diagnostics/logs/OID/tools/obckup.replicaid_pilot.TO.replicaid_ma
ster.timestamp.ldif.
Metadata copied successfully.
```

The output contains the expanded path `ORACLE_INSTANCE`.

---

**Note:** If Oracle Delegated Administration Services is not configured, then you might see an error message similar to this when you run remtool with the `-backupmetadata` option:

```
Failed to add "orclApplicationCommonName=ias.acme.com,
cn=IAS Instances, cn=IAS, cn=Products, cn=OracleContext"
as "uniquemember" to entry "cn=Associated Mid-tiers,
orclapplicationcommonname=DASApp, cn=DAS,cn=products,
cn=OracleContext at replica ldap://myhost:3060
```

Please ignore this error message.

---

**4.3.10.3.2 Backing Up the Metadata of a Pilot Replica to an LDIF File** This example shows how to back up the metadata entries for a pilot replica into an LDIF file.

**Example:**

```
remtool -backupmetadata -replica mypilot.company.com:3060 \
  -bkup /home/myfiles/obckup.ldif
```

The output from this command is:

```
Backup of metadata will be stored in /home/myfiles/obckup.ldif
Metadata copied successfully
```

## 4.3.11 The remtool -chgpwd Operation

The `chgpwd` operation is used to change the replication administrator password for an Oracle Database Advanced Replication-based directory replication group (DRG) that has already been setup using `asrsetup`.

The replication administrator password is the same for all nodes in an Advanced Replication DRG. This operation changes the password for all nodes in the DRG.

### 4.3.11.1 Syntax for remtool -chgpwd

```
remtool -chgpwd [-connect repl_admin_name@net_service_name] [-v]
```

### 4.3.11.2 Arguments for remtool -chgpwd

The tool also prompts you to enter the new password for the replication administrator.

**-connect repl\_admin\_name@net\_service\_name**

For more information, see [Section 4.3.31, "The -connect Connection Argument."](#)

### 4.3.11.3 Tasks and Examples for remtool -chgpwd

Using the `chgpwd` operation you can perform the following task:

- Section 4.3.11.3.1, "Changing the Administrator Password for an Advanced Replication-based DRG"

**4.3.11.3.1 Changing the Administrator Password for an Advanced Replication-based DRG** In this example, the password of the replication administrator of a DRG consisting of MY\_HOST1.MY\_COMPANY.COM and MY\_HOST2.MY\_COMPANY.COM is changed.

**Example:**

```
remtool -chgpwd -v -conn repadmin@MY_HOST1.MY_COMPANY.COM
```

The results are:

```
MY_HOST1.MY_COMPANY.COM is Master Definition Site (MDS). Connected to MDS.
MY_HOST2.MY_COMPANY.COM is Remote Master Site (RMS). Connected to RMS.
Directory Replication Group (DRG) details :
```

```
-----
Instance Host Name      Global Name              Version      ReplicaId    Site
Name                                                            Type
-----
rid1      my_host      MY_HOST1.MY_COMPANY.COM 10.1.2.0.0  my_host_rid1  MDS
rid2      my_host      MY_HOST2.MY_COMPANY.COM 10.1.2.0.0  my_host_rid2  RMS
-----
```

```
Enter new password of the replication administrator :
Reenter new password of the replication administrator :
```

```
-----
Changing the password of all nodes...
```

```
MY_HOST1.MY_COMPANY.COM : Changing password of replication administrator
repadmin...
MY_HOST2.MY_COMPANY.COM : Changing password of replication administrator
repadmin...
MY_HOST1.MY_COMPANY.COM : Dropping database link made to
MY_HOST2.MY_COMPANY.COM...
MY_HOST1.MY_COMPANY.COM : Dropping database link made to
MY_HOST2.MY_COMPANY.COM...
MY_HOST1.MY_COMPANY.COM : Creating database link to MY_HOST2.MY_COMPANY.COM...
MY_HOST2.MY_COMPANY.COM : Dropping database link made to
MY_HOST1.MY_COMPANY.COM...
MY_HOST2.MY_COMPANY.COM : Dropping database link made to
MY_HOST1.MY_COMPANY.COM...
MY_HOST2.MY_COMPANY.COM : Creating database link to MY_HOST1.MY_COMPANY.COM...
```

```
-----
Password has been changed.
-----
```

## 4.3.12 The remtool -delnode Operation

The delnode operation removes a remote master site (RMS) node from an existing directory replication group (DRG). You must first create the DRG using [Section 4.3.8, "The remtool -asrsetup Operation."](#) The following usage rules apply to this operation:

- You can only delete RMS nodes from a DRG, not the master definition site (MDS).
- Oracle Internet Directory processes on the master definition site (MDS) and other remote master sites (RMSs) in the DRG must be stopped before running the operation.
- If the RMS node being deleted is down when the delnode operation is invoked, it is selected for deletion.

- After the delnode operation is complete, Oracle Internet Directory processes can be restarted.

#### 4.3.12.1 Syntax for remtool -delnode

```
remtool -delnode [-connect repl_admin_name@net_service_name] [-v]
```

#### 4.3.12.2 Arguments for remtool -delnode

The tool also prompts you for the global database name (as defined in the tnsnames.ora file of the RMS node to be deleted from the DRG.

#### **-connect repl\_admin\_name@net\_service\_name**

For more information, see [Section 4.3.31, "The -connect Connection Argument."](#)

#### 4.3.12.3 Tasks and Examples for remtool -delnode

Using the delnode operation you can perform the following task:

- [Section 4.3.12.3.1, "Removing a RMS Node from an Advanced Replication-Based DRG"](#)

**4.3.12.3.1 Removing a RMS Node from an Advanced Replication-Based DRG** In this example, MY\_HOST3.MY\_COMPANY.COM is removed from a DRG consisting of MY\_HOST1.MY\_COMPANY.COM, MY\_HOST2.MY\_COMPANY.COM and MY\_HOST3.MY\_COMPANY.COM

#### **Example:**

```
remtool -delnode -v -conn repadmin@MY_HOST1.MY_COMPANY.COM
```

The results are:

```
MY_HOST1.MY_COMPANY.COM is Master Definition Site (MDS). Connected to MDS.
MY_HOST2.MY_COMPANY.COM is Remote Master Site (RMS). Connected to RMS.
MY_HOST3.MY_COMPANY.COM is Remote Master Site (RMS). Connected to RMS.
Directory Replication Group (DRG) details :
```

```
-----
Instance Host Name      Global Name              Version      ReplicaId      Site
Name                                                    Type
-----
rid1      my_host                 MY_HOST1.MY_COMPANY.COM  OID 10.1.2.0.0  my_host_rid1   MDS
rid2      my_host                 MY_HOST2.MY_COMPANY.COM  OID 10.1.2.0.0  my_host_rid2   RMS
rid3      my_host                 MY_HOST3.MY_COMPANY.COM  OID 10.1.2.0.0  my_host_rid3   RMS
-----
```

```
Do you want to continue? [y/n] : y
```

```
Enter globalname of node to be deleted : MY_HOST3.MY_COMPANY.COM
```

```
-----
Deleting an existing node...
```

```
MY_HOST1.MY_COMPANY.COM : Dropping replication site MY_HOST3.MY_COMPANY.COM from
replication group LDAP_REP...
MY_HOST3.MY_COMPANY.COM : Dropping replication group LDAP_REP...
MY_HOST3.MY_COMPANY.COM : Unsheduling push job to MY_HOST1.MY_COMPANY.COM...
MY_HOST3.MY_COMPANY.COM : Unsheduling push job to MY_HOST2.MY_COMPANY.COM...
MY_HOST3.MY_COMPANY.COM : Dropping database link made to
MY_HOST1.MY_COMPANY.COM...
MY_HOST3.MY_COMPANY.COM : Dropping database link made to
MY_HOST2.MY_COMPANY.COM...
```



```

MY_HOST3.MY_COMPANY.COM : Dropping database link made to
MY_HOST1.MY_COMPANY.COM...
MY_HOST3.MY_COMPANY.COM : Dropping database link made to
MY_HOST2.MY_COMPANY.COM...
Enter "SYSTEM" user password for "MY_HOST3.MY_COMPANY.COM" database at "my_host"
host :
MY_HOST3.MY_COMPANY.COM : Dropping replication administrator repadmin...
MY_HOST1.MY_COMPANY.COM : Unsheduling push job to MY_HOST3.MY_COMPANY.COM...
MY_HOST1.MY_COMPANY.COM : Dropping database link made to
MY_HOST3.MY_COMPANY.COM...
MY_HOST1.MY_COMPANY.COM : Dropping database link made to
MY_HOST3.MY_COMPANY.COM...
MY_HOST2.MY_COMPANY.COM : Unsheduling push job to MY_HOST3.MY_COMPANY.COM...
MY_HOST2.MY_COMPANY.COM : Dropping database link made to
MY_HOST3.MY_COMPANY.COM...
MY_HOST2.MY_COMPANY.COM : Dropping database link made to
MY_HOST3.MY_COMPANY.COM...
MY_HOST1.MY_COMPANY.COM : Verifying uniqueness of replication agreement entry...
MY_HOST2.MY_COMPANY.COM : Verifying uniqueness of replication agreement entry...
MY_HOST1.MY_COMPANY.COM : Verifying replication agreement entry...
MY_HOST1.MY_COMPANY.COM : Deleting replication agreement entry my_host_rid3...
CORRECTED:
MY_HOST1.MY_COMPANY.COM : "my_host_rid3" hostname has been removed from
replication agreement entry as it is not part of DRG or was repeated.
MY_HOST2.MY_COMPANY.COM : Verifying replication agreement entry...
MY_HOST2.MY_COMPANY.COM : Deleting replication agreement entry my_host_rid3...
CORRECTED:
MY_HOST2.MY_COMPANY.COM : "my_host_rid3" hostname has been removed from
replication agreement entry as it is not part of DRG or was repeated.
-----
Node MY_HOST3.MY_COMPANY.COM has been deleted from this DRG.
-----
Directory Replication Group (DRG) details :

-----
Instance Host Name      Global Name              Version      ReplicaId      Site
Name                                     Type
-----
rid1      my_host                 MY_HOST1.MY_COMPANY.COM 10.1.2.0.0  my_host_rid1  MDS
rid2      my_host                 MY_HOST2.MY_COMPANY.COM 10.1.2.0.0  my_host_rid2  RMS
-----
=====

```

### 4.3.13 The remtool -dispasrerr Operation

The `dispasrerr` operation displays errors for an Oracle Database Advanced Replication-based directory replication group (DRG). It shows both administrative request errors and deferred transaction errors.

#### 4.3.13.1 Syntax for remtool -dispasrerr

```
remtool -dispasrerr [-connect repl_admin_name@net_service_name] [-v]
```

#### 4.3.13.2 Arguments for remtool -dispasrerr

**-connect repl\_admin\_name@net\_service\_name**

For more information, see [Section 4.3.31, "The -connect Connection Argument."](#)

### 4.3.13.3 Tasks and Examples for remtool -dispsrerr

Using the dispsrerr operation you can perform the following task:

- [Section 4.3.13.3.1, "Displaying Errors for an Oracle Database Advanced Replication-based DRG"](#)

**4.3.13.3.1 Displaying Errors for an Oracle Database Advanced Replication-based DRG** In this example, the tool reports Advanced Replication errors for a DRG consisting of MY\_HOST1.MY\_COMPANY.COM and MY\_HOST2.MY\_COMPANY.COM.

#### Example:

```
remtool -dispsrerr -v -conn repadmin@my_host1.my_company.com
```

```
MY_HOST1.MY_COMPANY.COM is Master Definition Site (MDS). Connected to MDS.
```

```
MY_HOST2.MY_COMPANY.COM is Remote Master Site (RMS). Connected to RMS.
```

```
Directory Replication Group (DRG) details :
```

```
-----
Instance Host Name      Global Name              Version      ReplicaId    Site
Name                                                           Type
-----
rid      my_host      MY_HOST1.MY_COMPANY.COM  OID 10.1.2.0.0  my_host_rid1  MDS
rid2     my_host      MY_HOST2.MY_COMPANY.COM  OID 10.1.2.0.0  my_host_rid2  RMS
-----
```

```
Following administrative request errors were found at MY_HOST1.MY_COMPANY.COM
```

```
-----
Admin request      Request raised at      Error
raised by
-----
REPADMIN           MY_HOST1.MY_COMPANY.  ORA-23309: object ODS.ASR_CHG_L
REPADMIN           MY_HOST1.MY_COMPANY.  ORA-23309: object ODS.ODS_CHG_S
REPADMIN           MY_HOST1.MY_COMPANY.  ORA-23416: table "ODS"."ODS_CHG
REPADMIN           MY_HOST1.MY_COMPANY.  ORA-23308: object ODS.ODS_CHG_S
REPADMIN           MY_HOST1.MY_COMPANY.  ORA-23416: table "ODS"."ASR_CHG
REPADMIN           MY_HOST1.MY_COMPANY.  ORA-23308: object ODS.ASR_CHG_L
-----
```

```
Following deferred transaction errors were found at MY_HOST1.MY_COMPANY.COM
```

```
-----
Deferred          Deferred Trans  Destination      Error
Transaction ID    Origin DB
-----
1.2.3733          MY_HOST1.MY_COM  MY_HOST1.MY_COM  ORA-01403: no data found
-----
```

```
No deferred transaction errors were found at MY_HOST2.MY_COMPANY.COM
-----
```

### 4.3.14 The remtool -dispqstat Operation

The dispqstat operation displays the queue statistics for a directory replication group (DRG) that uses Oracle Database Advanced Replication. This operation cannot be used for DRGs that use LDAP-based replication. If a DRG uses both Advanced and

LDAP-based replication, this operation displays queue statistics for nodes that use Advanced Replication only.

#### 4.3.14.1 Syntax for remtool -dispqstat

```
remtool -dispqstat [-connect repl_admin_name@net_service_name] [-v]
```

#### 4.3.14.2 Arguments for remtool -dispqstat

##### **-connect repl\_admin\_name@net\_service\_name**

The connection string for the master definition site (MDS) or the Remote Master Site (RMS). You are prompted for the password for the replication administrator. If you do not supply an argument on the command-line, the tool prompts you for the information. The connect string is composed of the following elements:

- The name of the replication administrator.
- The net service name of the MDS or RMS. If you have a `tnsnames.ora` file configured, then this is the net service name specified in that file, which is located by default in `ORACLE_INSTANCE/config`. (You can set the `TNS_ADMIN` environment variable if you want to use a different location.)

#### 4.3.14.3 Tasks and Examples for remtool -dispqstat

Using the `dispqstat` operation you can perform the following tasks:

- [Section 4.3.14.3.1, "Displaying Queue Statistics for an Advanced Replication-Based DRG"](#)

**4.3.14.3.1 Displaying Queue Statistics for an Advanced Replication-Based DRG** In this example, queue statistics for an Oracle Database Advanced Replication-based DRG consisting of `MY_HOST1.MY_COMPANY.COM` and `MY_HOST2.MY_COMPANY.COM` are reported.

##### **Example:**

```
remtool -dispqstat -v -conn repadmin@my_host1.my_company.com
```

The results are:

```
MY_HOST1.MY_COMPANY.COM is Master Definition Site (MDS). Connected to MDS.
MY_HOST2.MY_COMPANY.COM is Remote Master Site (RMS). Connected to RMS.
Directory Replication Group (DRG) details :
```

```
-----
Instance Host Name      Global Name              Version      ReplicaId      Site
Name                                                           Type
-----
rid1    my_host      MY_HOST1.MY_COMPANY.COM 10.1.2.0.0  my_host_rid1  MDS
rid2    my_host      MY_HOST2.MY_COMPANY.COM 10.1.2.0.0  my_host_rid2  RMS
-----
```

Queue Statistics :

```
-----
Supplier      Consumer      New      Retry      Purge      HIQ      Change #
-----
MY_HOST1.MY CO MY_HOST1.MY CO      3         9         10         6         2003
MY_HOST1.MY CO MY_HOST2.MY CO      2         7         8          5         2001
MY_HOST2.MY CO MY_HOST1.MY CO      2         8         5          8         2002
MY_HOST2.MY CO MY_HOST2.MY CO      2        10         7          8         2000
-----
```

Legends

New: No. of new change logs  
 Retry: No. of change logs in retry queue  
 Purge: No. of change logs in purge queue  
 HIQ: No. of change logs in Human Intervention Queue (HIQ)  
 Change # : Last applied change log no.

### 4.3.15 The remtool -paddnode Operation

The `paddnode` operation adds a replica or partial replica to a directory replication group (DRG). This operation has the following usage rules:

- The supplier node (the master copy) can be part of a DRG that uses Advanced Replication, LDAP-based replication, or both.
- If you want to specify a supplier node that uses Advanced Replication, you must bind using that node's connection information.
- The new replica to be added should not be a member of any DRG.
- A consumer node (the destination of replication updates) can be any node that uses LDAP-based replication.
- After adding a replica, you can choose the naming context(s) to participate in replication, or choose the entire directory by selecting \* (asterisk). Choosing specific naming contexts replicates only that portion of the directory. Choosing the entire directory replicates all directory data except for directory-specific entries (DSE).
- The `cn=oraclecontext` naming context is included for replication whether or not any naming contexts are specified by the user.

#### 4.3.15.1 Syntax for remtool -paddnode

```
remtool -paddnode [-bind supplier_hostname:ldap_port] [-v]
```

#### 4.3.15.2 Arguments for remtool -paddnode

You are prompted for the password for the replication DN on the consumer node. You are prompted for the following arguments if you do not specify them:

- **Consumer Host Name of Host Running OID Server** - The host name of the Oracle Internet Directory server where you want to create the replica. This node can be added to the DRG as a read-only or updateable replica.
- **Consumer Port** - The LDAP listening port of the consumer node.

In addition, the tool prompts you for the following information:

- **Replica ID of Supplier** - If the DRG contains multiple nodes that can be used as the supplier, you are prompted to enter the replica ID of the one you want to use.
- **Naming Context** - For a partial replica, you can enter the name(s) of the naming context you want to replicate. To select the entire directory, enter \* (asterisk). To select none, enter e (end).

#### **-bind supplier\_hostname:ldap\_port**

See [Section 4.3.30, "The -bind Connection Argument"](#) for information.

#### 4.3.15.3 Tasks and Examples for remtool -paddnode

Using the `paddnode` operation you can perform the following tasks:

- [Section 4.3.15.3.1, "Adding a Read-Only Replica to a DRG"](#)

- Section 4.3.15.3.2, "Adding a Partial Replica to a DRG"

**4.3.15.3.1 Adding a Read-Only Replica to a DRG** In this example, directory server `ldap://my_host:3060` is added as a replica to directory server `ldap://my_host:3040`, which is part of the DRG consisting of `ldap://my_host:3040` and `ldap://my_host:3080`, which both use LDAP-based replication.

**Example:**

```
remtool -paddnode -v -bind my_host:3040
```

The results are:

Directory Replication Group (DRG) details :

```
-----
Sl  ReplicaId          Directory Information  Supplier Information  Repl.
No.                                                                Type
-----
001 my_host_rid1      my_host:3040         --                    RW
002 my_host_rid3      my_host:3080         my_host_rid1         RO
-----
```

Enter consumer directory details:

Enter hostname of host running OID server : my\_host

Enter port on which OID server is listening : 3060

Enter replication dn password :

Enter replica type [1 - LDAP read-only replica; 2 - LDAP updateable replica] : 1

Enter replicaId of the supplier : my\_host\_rid1

```
-----
ldap://my_host:3060 [my_host_r[my_host_rid1]id2] : Modifying entry
orclreplicaId=my_host_rid2,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Modifying entry ...
ldap://my_host:3040 [my_host_rid1] : Modifying entry
orclreplicaId=my_host_rem,cn=replication configuration...
ldap://my_host:3040 [my_host_rid1] : Modifying entry ...
ldap://my_host:3040 [my_host_rid1] : Modifying entry ...
ldap://my_host:3040 [my_host_rid1] : Adding entry
orclagreementId=000003,orclreplicaId=my_host_rid,cn=replication configuration...
ldap://my_host:3040 [my_host_rid1] : Adding entry
orclreplicaId=my_host_rem2,cn=replication configuration...
ldap://my_host:3040 [my_host_rid1] : Adding entry cn=replication
dn,orclreplicaId=my_host_rem2,cn=replication configuration...
ldap://my_host:3080 [my_host_rid3] : Adding entry
orclreplicaId=my_host_rem2,cn=replication configuration...
ldap://my_host:3080 [my_host_rid3] : Adding entry cn=replication
dn,orclreplicaId=my_host_rem2,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Adding entry
orclreplicaId=my_host_rem,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Adding entry
orclagreementId=000002,orclreplicaId=my_host_rem,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Adding entry
orclagreementId=000003,orclreplicaId=my_host_rid,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Adding entry cn=replication
dn,orclreplicaId=my_host_rid,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Adding entry
orclreplicaId=my_host_rem3,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Adding entry cn=replication
```

```
dn,orclreplicaid=my_host_rid3,cn=replication configuration...
ldap://my_host:3080 [my_host_rid3] : Adding entry
orclagreementid=000003,orclreplicaid=my_host_rid,cn=replication configuration...
```

```
-----
Replica ldap://my_host:3060(my_host_rem2) has been added to this DRG.
-----
```

```
Directory Replication Group (DRG) details :
```

```
-----
S1  Replicaid          Directory Information  Supplier Information  Repl.
No.                                                                Type
-----
001 my_host_rid1      my_host:3040          --                    RW
002 my_host_rid2      my_host:3060          my_host_rid1         RO
003 my_host_rid3      my_host:3080          my_host_rid1         RO
-----
```

```
-----
Replica ldap://my_host:3060 (my_host_rid2) can be made partial replica by
specifying naming contexts to be replicated.
-----
```

```
List of available naming contexts in supplier replica ldap://my_host:3040
(my_host_rid1) :
```

```
1. * [replicate whole directory]
Enter naming context (e-end, q-quit) : e
-----
-----
```

**4.3.15.3.2 Adding a Partial Replica to a DRG** In this example, the directory server ldap://my\_host:3060 is added as a partial replica by specifying the naming contexts to be replicated to directory server ldap://my\_host:3040.

**Example:**

```
remtool -paddnode -v -bind my_host:3040
```

The results are:

```
Directory Replication Group (DRG) details :
```

```
-----
S1  Replicaid          Directory Information  Supplier Information  Repl.
No.                                                                Type
-----
001 my_host_rid      my_host:3040          --                    RW
-----
```

```
Enter consumer directory details:
```

```
Enter hostname of host running OID server      : my_host
```

```
Enter port on which OID server is listening   : 3060
```

```
Enter replication dn password                  :
```

```
Enter replica type [1 - LDAP read-only replica; 2 - LDAP updateable replica] : 2
-----
```

```
ldap://my_host:3060 [my_host_rid2] : Modifying entry
```

```

orclreplicaid=my_host_rid2,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Modifying entry ...
ldap://my_host:3040 [my_host_rid1] : Modifying entry
orclreplicaid=my_host_rid1,cn=replication configuration...
ldap://my_host:3040 [my_host_rid1] : Modifying entry ...
ldap://my_host:3040 [my_host_rid1] : Modifying entry ...
ldap://my_host:3040 [my_host_rid1] : Adding entry
orclagreementid=000002,orclreplicaid=my_host_rid1,cn=replication configuration...
ldap://my_host:3040 [my_host_rid1] : Adding entry
orclreplicaid=my_host_rid2,cn=replication configuration...
ldap://my_host:3040 [my_host_rid1] : Adding entry cn=replication
dn,orclreplicaid=my_host_rid2,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Adding entry
orclreplicaid=my_host_rid1,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Adding entry
orclagreementid=000002,orclreplicaid=my_host_rid1,cn=replication configuration...
ldap://my_host:3040 [my_host_rid] : Adding entry
cn=includednamingcontext000001,orclagreementid=000002,orclreplicaid=usunnae07_prep
,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Adding entry
cn=includednamingcontext000001,orclagreementid=000002,orclreplicaid=usunnae07_prep
,cn=replication configuration...

```

```

-----
Replica ldap://my_host:3060(my_host_rid2) has been added to this DRG.
-----

```

Directory Replication Group (DRG) details :

Sl No.	Replicaid	Directory Information	Supplier Information	Repl. Type
001	my_host_rid1	my_host:3040	--	RW
002	my_host_rid2	my_host:3060	my_host_rid1	RW

```

-----
Replica ldap://my_host:3060 (my_host_rem2) can be made partial replica by
specifying naming contexts to be replicated.
-----

```

```

-----
List of available naming contexts in supplier replica ldap://my_host:3040
(my_host_rid1) :

```

1. \* [replicate whole directory]
2. dc=com
3. dc=org
4. dc=net
5. dc=edu

Enter naming context (e-end, q-quit) : dc=org

Enter naming context (e-end, q-quit) : dc=edu

Enter naming context (e-end, q-quit) : e

Following naming contexts will be included for replication:

1. dc=org
2. dc=edu

Do you want to continue? [y/n] : y

```

ldap://my_host:3040 [my_host_riid1] : Adding entry
cn=includednamingcontext000002,orclagreementid=000002,orclreplicaid=my_host_riid,cn
=replication configuration...
ldap://my_host:3060 [my_host_riid2] : Adding entry
cn=includednamingcontext000002,orclagreementid=000002,orclreplicaid=my_host_riid,cn
=replication configuration...
ldap://my_host:3040 [my_host_riid1] : Adding entry
cn=includednamingcontext000003,orclagreementid=000002,orclreplicaid=my_host_riid,cn
=replication configuration...
ldap://my_host:3060 [my_host_riid2] : Adding entry
cn=includednamingcontext000003,orclagreementid=000002,orclreplicaid=my_host_riid,cn
=replication configuration...

```

```

-----
Selected naming contexts have been included for replication.
-----

```

## 4.3.16 The remtool -pdisplay Operation

The `pdisplay` operation displays all replica details in a partial replication group.

### 4.3.16.1 Arguments to remtool -pdisplay

**-bind supplier\_hostname:ldap\_port**

See [Section 4.3.30, "The -bind Connection Argument"](#) for information.

## 4.3.17 The remtool -pchgmaster Operation

The `pchgmaster` operation is used to break the agreement with the old supplier and reestablish the agreement with a new supplier. This operation is part of configuring replication failover.

**See Also:** "Configuring Replication Failover" in *Oracle Internet Directory Administrator's Guide* for details on performing the replication failover process

The `pchgmaster` operation has the following usage rules:

1. If you do not supply consumer directory details using the `-bind` option, then you are prompted to specify consumer details.
2. If the consumer details are valid, then `remtool` identifies all nodes in the DRG, if any, and displays their details.
3. You are next prompted for the retiring and new supplier details.
4. After the change master operation completes successfully, you might need to use `remtool -pcleanup -agrmt` on the old supplier to remove the old agreement. This would be the case if the old supplier was offline during the change master operation. See [Section 4.3.20, "The remtool -pcleanup Operation"](#) for details about the `pcleanup` operation.

### 4.3.17.1 Syntax for remtool -pchgmaster

```
remtool -pchgmaster [-bind replica_hostname:ldap_port] [ multimaster ] [-v]
```



### 4.3.17.2 Arguments for remtool -pchgmaster

The tool prompts you for the host names and port numbers of the retiring supplier and the new supplier.

#### **-bind replica\_hostname:port\_number**

See Section 4.3.30, "The -bind Connection Argument" for information.

#### **-multimaster**

This suboption causes changeMaster to change the primary replica in a multimaster agreement.

### 4.3.17.3 Tasks and Examples for remtool -pchgmaster

Using the pchgmaster operation, you can perform the following tasks:

- Section 4.3.17.3.1, "Breaking a Supplier Agreement and Creating a New One for a Consumer"

**4.3.17.3.1 Breaking a Supplier Agreement and Creating a New One for a Consumer** In this example, the supplier of directory server ldap://my\_host:3060 is changed from directory server ldap://my\_host:3040 to directory server ldap://my\_host:3080.

#### **Example:**

```
remtool -pchgmaster -v -bind my_host:3060
```

The results are:

Directory Replication Group (DRG) details :

```
-----
S1   ReplicaId      Directory Information   Supplier Information   Repl.
No.                                     my_host_rid1          Type
-----
001 my_host_rid2    my_host:3060           my_host_rid1          RW
002 my_host_rid3    my_host:3080           my_host_rid1          RW
003 my_host_rid1    my_host:3040           my_host_rid3          RW
                                     my_host_rid2
-----

Enter replica ID of the retiring supplier      : my_host_rid1
-----
Enter hostname of the new supplier             : my_host

Enter port number of the new supplier          : 3080
Enter replication DN password of the new supplier :
* WARNING *: Moving my_host_rid1 to be consumer of my_host_rid3 might cause
discrepancy in data.
Do you want to continue? [y/n]: y
ldap://my_host:3060 [my_host_rid2] : Modifying entry
orclagreementid=000003,orclreplicaid=my_host_rid1,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Modifying entry
orclagreementid=000003,orclreplicaid=my_host_rid1,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Adding entry
orclreplicaid=my_host_rid3,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Adding entry cn=replication
```

```

dn,orclreplicaid=my_host_rid3,cn=replication configuration...
ldap://my_host:3080 [my_host_rid3] : Deleting entry
orclagreementid=000003,orclreplicaid=my_host_rid1,cn=replication configuration...
ldap://my_host:3080 [my_host_rid3] : Adding entry
orclreplicaid=my_host_rid2,cn=replication configuration...
ldap://my_host:3080 [my_host_rid3] : Adding entry cn=replication
dn,orclreplicaid=my_host_rid2,cn=replication configuration...
ldap://my_host:3080 [my_host_rid3] : Adding entry
orclagreementid=000004,orclreplicaid=my_host_rid3,cn=replication configuration...
ldap://my_host:3080 [my_host_rid3] : Adding entry cn=replication
namecontext,orclagreementid=000004,orclreplicaid=my_host_rid3,cn=replication
configuration...
ldap://my_host:3080 [my_host_rid3] : Adding entry
cn=includednamingcontext000002,cn=replication
namecontext,orclagreementid=000004,orclreplicaid=my_host_rid3,cn=replication
configuration...
ldap://my_host:3080 [my_host_rid3] : Adding entry
cn=includednamingcontext000001,cn=replication
namecontext,orclagreementid=000004,orclreplicaid=my_host_rid3,cn=replication
configuration...
ldap://my_host:3080 [my_host_rid3] : Modifying entry ...
ldap://my_host:3040 [my_host_rid1] : Deleting entry
orclagreementid=000003,orclreplicaid=my_host_rid1,cn=replication configuration...

```

-----  
Directory Replication Group (DRG) details :

S1 No.	Replicaid	Directory Information	Supplier Information	Repl. Type
001	my_host_rid2	my_host:3060	my_host_rid3	RW
002	my_host_rid3	my_host:3080	my_host_rid1 my_host_rid2	RW
003	my_host_rid1	my_host:3040	my_host_rid3	RW

-----  
Change master of my\_host\_rid2 to my\_host\_rid3 successfully.

**4.3.17.3.2 Changing the Primary Node** In this example, the primary node in a three-node LDAP multimaster agreement is changed from stacu14\_tst1 to stacu14\_tst13

**Example:**

```
remtool -pchgmaster -multimaster
```

The result is:

-----  
Directory Replication Group (DRG) details :

S1 No.	Replicaid	Directory Information	Supplier Information	Repl. Type
001	stacu14_tst1	stacu14:3069	stacu14_tst13 stacu14_tst12	RW
002	stacu14_tst13	stacu14:3089	stacu14_tst12 stacu14_tst1	RW
003	stacu14_tst12	stacu14:3079	stacu14_tst13 stacu14_tst1	RW

```

-----
Enter new primary replica ID      : stacul4_tst13

Changed primary replica from stacul4_tst1 to stacul4_tst13 successfully.

```

## 4.3.18 The remtool -pchgpwd Operation

This `pchgpwd` operation changes the replication DN password for an Oracle Internet Directory server. The password is changed in both the directory and in wallet.

If the replica is taking part in replication, the password is changed in other replicas for the local replica's replication DN. Note that, unlike Advanced Replication, the replication DN password for each replica can be different.

The operation must be run on the host of the Oracle Internet Directory server whose password you are changing in order to update the wallet password at the same time. You can also update the wallet password separately using [Section 4.3.19, "The remtool -pchgwalpwd Operation."](#)

### 4.3.18.1 Syntax for remtool -pchgpwd

```
remtool -pchgpwd [-bind oid_hostname:ldap_port] [-v]
```

### 4.3.18.2 Arguments for remtool -pchgpwd

In addition to the arguments specified on the command-line, the tool also prompts you for the new replication DN password for the host specified in the bind connection string.

#### **-bind supplier\_hostname:ldap\_port**

See [Section 4.3.30, "The -bind Connection Argument"](#) for information.

### 4.3.18.3 Tasks and Examples for remtool -pchgpwd

Using the `pchgpwd` operation you can perform the following tasks:

- [Section 4.3.18.3.1, "Changing the Replication DN Password Used for LDAP-Based Replication"](#)

**4.3.18.3.1 Changing the Replication DN Password Used for LDAP-Based Replication** In this example, the replication DN password of the Oracle Internet Directory server `ldap://my_host:3040` is changed.

#### **Example:**

```
remtool -pchgpwd -v -bind my_host:3040
```

The results are:

```
Directory Replication Group (DRG) details :
```

```

-----
Sl  ReplicaId      Directory Information  Supplier Information  Repl.
No.
-----
001 my_host_rid1   my_host:3040          --                    RW
002 my_host_rid3   my_host:3080          my_host_rid1         RO
-----

```

```

-----
Replication DN password of ldap://my_host:3040 (my_host_rem) associated with
database 'rid' will be changed.
Do you want to continue? [y/n] : y

Enter new password of replication DN      :
Reenter new password of replication DN    :

-----
ldap://my_host:3040 [my_host_rid1] : Modifying entry cn=replication
dn,orclreplicaid=my_host_rem,cn=replication configuration...
ldap://my_host:3080 [my_host_rid3] : Modifying entry cn=replication
dn,orclreplicaid=my_host_rem,cn=replication configuration...

-----
Password has been changed.
-----

```

### 4.3.19 The remtool -pchgwalpwd Operation

The `pchgwalpwd` operation is used to change the replication DN password only in the wallet of an Oracle Internet Directory server. It sets the wallet password to the same replication DN password stored in the Oracle Internet Directory repository for the host specified in the bind connection string.

#### 4.3.19.1 Syntax for remtool -pchgwalpwd

```
remtool -pchgwalpwd [-bind oid_hostname:ldap_port] [-v]
```

#### 4.3.19.2 Arguments for remtool -pchgwalpwd

##### **-bind supplier\_hostname:ldap\_port**

See [Section 4.3.30, "The -bind Connection Argument"](#) for information.

#### 4.3.19.3 Tasks and Examples for remtool -pchgwalpwd

Using the `pchgwalpwd` operation you can perform the following task:

- [Section 4.3.19.3.1, "Changing the Replication DN Password in the Oracle Internet Directory Wallet"](#)

**4.3.19.3.1 Changing the Replication DN Password in the Oracle Internet Directory Wallet** In this example, the replication DN password for Oracle Internet Directory server `ldap://my_host:3040` is set in wallet to match the password in the repository.

##### **Example:**

```
remtool -pchgwalpwd -v -bind my_host:3040
```

The results are:

Directory Replication Group (DRG) details :

```

-----
S1  Replicaid          Directory Information  Supplier Information  Repl.
No.                                     Type
-----
001 my_host_rid1      my_host:3040          --                    RW
002 my_host_rid3      my_host:3080          my_host_rid1         RO
-----

```

```
-----
Replication DN password of ldap://my_host:3040 (my_host_rid1) associated with
database 'rid' will be set in wallet.
Do you want to continue? [y/n] : y
```

## 4.3.20 The remtool -pcleanup Operation

The `pcleanup` operation is used to clean up an LDAP-based directory replication group (DRG) setup. It cleans up a replica which has incomplete or flawed LDAP-based DRG setup. It only cleans up the replica identified by the bind connection string.

If replication configuration information is corrupted, or the replication DN entry is not available, then the tool prompts for the Oracle Internet Directory superuser DN and password.

This operation only cleans up LDAP-based DRG setup. For clean up of an Oracle Database Advanced Replication-based DRG setup, see [Section 4.3.6, "The remtool -asrcleanup Operation"](#).

### 4.3.20.1 Syntax for remtool -pcleanup

```
remtool -pcleanup [-bind oid_hostname:ldap_port] [-agrmt] [-v]
```

### 4.3.20.2 Arguments for remtool -pcleanup

#### -bind supplier\_hostname:ldap\_port

See [Section 4.3.30, "The -bind Connection Argument"](#) for information.

#### -agrmt

Optional. Use this option to clean up dead LDAP agreements at a node. Dead agreements might exist if:

- A node in the DRG was offline when you ran `remtool -pcleanup`.
- The node being deleted was offline when you ran `remtool -delnode`.
- The supplier node was offline when you ran `remtool -pchgmaster`.

Alternatively, in the first two cases, you could run `remtool -pcleanup` (without `-agrmt`) to delete all the agreements.

### 4.3.20.3 Tasks and Examples for remtool -pcleanup

Using the `pcleanup` operation you can perform the following tasks:

- [Section 4.3.20.3.1, "Cleaning Up an Incomplete or Flawed LDAP-based DRG Setup"](#)
- [Section 4.3.20.3.2, "Cleaning Up Specific LDAP Agreements"](#)

**4.3.20.3.1 Cleaning Up an Incomplete or Flawed LDAP-based DRG Setup** In this example, the tool cleans up the replication setup of a DRG that has three replicas taking part in LDAP based replication.

#### Example:

```
remtool -pcleanup -v -bind my_host:3040
```

The results are:

Directory Replication Group (DRG) details :

Sl No.	Replicaid	Directory Information	Supplier Information	Repl. Type
001	my_host_rid1	my_host:3040	--	RW
002	my_host_rid3	my_host:3080	my_host_rid1	RO
003	my_host_rid2	my_host:3060	my_host_rid1	RO

DRG identified by replica ldap://my\_host:3040 (my\_host\_rid1) will be cleaned up.  
Do you want to continue? [y/n] : y

```

ldap://my_host:3040 [my_host_rid1] : Modifying entry
orclreplicaid=my_host_rem,cn=replication configuration...
ldap://my_host:3040 [my_host_rid1] : Modifying entry ...
ldap://my_host:3040 [my_host_rid1] : Modifying entry ...
ldap://my_host:3040 [my_host_rid1] : Deleting entry
orclagreementid=000002,orclreplicaid=my_host_rem,cn=replication configuration...
ldap://my_host:3040 [my_host_rid1] : Deleting entry
orclagreementid=000003,orclreplicaid=my_host_rem,cn=replication configuration...
ldap://my_host:3040 [my_host_rid1] : Deleting entry
orclreplicaid=my_host_rem3,cn=replication configuration...
ldap://my_host:3040 [my_host_rid1] : Deleting entry
orclreplicaid=my_host_rem2,cn=replication configuration...
ldap://my_host:3080 [my_host_rid3] : Modifying entry
orclreplicaid=my_host_rem3,cn=replication configuration...
ldap://my_host:3080 [my_host_rid3] : Modifying entry ...
ldap://my_host:3080 [my_host_rid3] : Modifying entry ...
ldap://my_host:3080 [my_host_rid3] : Deleting entry
orclreplicaid=my_host_rem,cn=replication configuration...
ldap://my_host:3080 [my_host_rid3] : Deleting entry
orclreplicaid=my_host_rem2,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Modifying entry
orclreplicaid=my_host_rem2,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Modifying entry ...
ldap://my_host:3060 [my_host_rid2] : Modifying entry ...
ldap://my_host:3060 [my_host_rid2] : Deleting entry
orclreplicaid=my_host_rem3,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Deleting entry cn=replication
dn,orclreplicaid=my_host_rem3,cn=replication configuration...

```

Replica ldap://my\_host:3040(my\_host\_rid1) has been cleaned up.

**4.3.20.3.2 Cleaning Up Specific LDAP Agreements** In this example, the agreement between directory servers ldap://my\_host:3040 and ldap://my\_host:3060 is cleaned up. The agreement between directory servers ldap://my\_host:3040 and ldap://my\_host:3080 is also cleaned up.

**Example:**

```
remtool -pcleanup -v -agrmt -bind my_host:3040
```

Directory Replication Group (DRG) details :

```

-----
Sl  ReplicaId          Directory Information  Supplier Information  Repl.
No.                                                                Type
-----
001  my_host_rid1       my_host:3040          my_host_rid2         RW
                               my_host_rid3

002  my_host_rid3       my_host:3080          my_host_rid1         RW

003  my_host_rid2       my_host:3060          my_host_rid1         RW
-----

Enter replica ID of replica(s) for which its(their) agreement(s) with replica
ldap://my_host:3040 (my_host_rid1) will be cleaned up.
Enter replica ID [Enter "e" to end selection] : my_host_rid2

Enter replica ID [Enter "e" to end selection] : my_host_rid3

Enter replica ID [Enter "e" to end selection] : e

-----
Agreement(s) with the following replica(s) would be cleaned up:
    0. my_host_rid2
    1. my_host_rid3
Do you want to continue? [y/n] : y

-----
Successfully cleaned up agreement between my_host_rid1 and my_host_rid2.
Successfully cleaned up agreement between my_host_rid1 and my_host_rid3.
-----
Replica ldap://my_host:3040(my_host_rid1) has been cleaned up.
-----

```

## 4.3.21 The remtool -pdelnode Operation

The `pdelnode` operation deletes an LDAP-based replica or partial replica from a directory replication group (DRG). To delete an Oracle Database Advanced Replication-based replica, used the [Section 4.3.21, "The remtool -pdelnode Operation"](#).

### 4.3.21.1 Syntax for remtool -pdelnode

```
remtool -pdelnode [-bind hostname:ldap_port] [-v]
```

### 4.3.21.2 Arguments for remtool -pdelnode

In addition to the arguments specified on the command-line, the tool prompts you for the following information:

- The replica ID of the replica to be deleted - The replica ID of the LDAP-based replica you want to delete.

#### **-bind hostname:ldap\_port**

See [Section 4.3.30, "The -bind Connection Argument"](#) for information.

### 4.3.21.3 Tasks and Examples for remtool -pdelnode

Using the `pdelnode` operation you can perform the following tasks:

- [Section 4.3.21.3.1, "Deleting a Read-Only Replica from a DRG"](#)

**4.3.21.3.1 Deleting a Read-Only Replica from a DRG** In this example, replica `ldap://my_host:3080` is removed from the DRG. This DRG consists of three replicas: `ldap://my_host:3040`, `ldap://my_host:3060`, and `ldap://my_host:3080`, of which `ldap://my_host:3040` and `ldap://my_host:3060` uses Advanced Replication and `ldap://my_host:3040` and `ldap://my_host:3080` uses LDAP-based replication. To delete replica `ldap://my_host:3080`, user has to give bind details of either `ldap://my_host:3040` or `ldap://my_host:3080`.

**Example:**

```
remtool -pdelnode -v -bind my_host:3040
-----
Directory Replication Group (DRG) details :
-----
Sl  ReplicaId          Directory Information  Supplier Information  Repl.
No.                                                            Type
-----
001 my_host_rid1       my_host:3040         my_host_rid2         RW
002 my_host_rid2     --                   my_host_rid1         RW
003 my_host_rid3     my_host:3080         my_host_rid1         RO
-----
Enter replicaId of the replica to be deleted : my_host_rid3
-----
ldap://my_host:3040 [my_host_rid1] : Modifying entry ...
ldap://my_host:3040 [my_host_rid1] : Deleting entry
orclagreementid=000002,orclreplicaId=my_host_rid1,cn=replication configuration...
ldap://my_host:3040 [my_host_rid1] : Deleting entry
orclreplicaId=my_host_rem3,cn=replication configuration...
ldap://my_host:3080 [my_host_rid3] : Modifying entry
orclreplicaId=my_host_rem3,cn=replication configuration...
ldap://my_host:3080 [my_host_rid3] : Modifying entry ...
ldap://my_host:3080 [my_host_rid3] : Deleting entry
orclreplicaId=my_host_rem,cn=replication configuration...
-----
Replica ldap://my_host:3080(my_host_rid3) has been deleted from this DRG.
-----
Directory Replication Group (DRG) details :
-----
Sl  ReplicaId          Directory Information  Supplier Information  Repl.
No.                                                            Type
-----
001 my_host_rid1       my_host:3040         my_host_rid2         RW
002 my_host_rid2     --                   my_host_rid1         RW
-----
```

## 4.3.22 The remtool -pdispqstat Operation

The `pdispqstat` operation displays the queue statistics for a directory replication group (DRG) that uses LDAP-based replication. This operation cannot be used for DRGs that use ASR-based (advanced) replication. If a DRG uses both ASR and LDAP-based replication, the `pdispqstat` operation displays queue statistics for nodes that use LDAP-based replication only.



---



---

**Note:** The `dispqstat` operation is used to display the queue statistics for a DRG that uses ASR-based replication.

---



---

**See Also:** [Section 4.3.14, "The remtool -dispqstat Operation"](#) for more details on displaying the queue statistics for a DRG that uses ASR-based replication

#### 4.3.22.1 Syntax for remtool -pdispqstat

```
remtool -pdispqstat [-bind hostname:ldap_port] [-v]
```

#### 4.3.22.2 Arguments for remtool -pdispqstat

##### -bind hostname:ldap\_port

See [Section 4.3.30, "The -bind Connection Argument"](#) for information.

#### 4.3.22.3 Tasks and Examples for remtool -pdispqstat

Using the `pdispqstat` operation, you can perform the following tasks:

- [Section 4.3.22.3.1, "Display queue statistics for LDAP-based replicas"](#)

**4.3.22.3.1 Display queue statistics for LDAP-based replicas** In this example, queue statistics for a DRG consisting of directory servers `ldap://my_host:3040` and `ldap://my_host:3060` are displayed.

##### Example:

```
remtool -pdispqstat -v -bind my_host:3040
```

Directory Replication Group (DRG) details :

```
-----
Sl   ReplicaId      Directory Information   Supplier Information   Repl.
No.                                     Type
-----
001  my_host_rid1     my_host:3040           my_host_rid2          RW
002  my_host_rid2     my_host:3060           my_host_rid1          RW
-----
```

Queue Statistics:

```
-----
Supplier      Consumer      PROTO New  Retry  Purge  HIQ  LA Chg#  Logs  TBP  LT Chg#
-----
my_host_rid2  my_host_rid1  LDAP  0   0     1     2   2001    0     2001
my_host_rid1  my_host_rid2  LDAP  0   0     2     3   2082    3     70335
-----
```

Legends:

```
New       : No. of new change logs
Retry     : No. of change logs in retry queue
Purge    : No. of change logs in purge queue
HIQ      : No. of change logs in Human Intervention Queue (HIQ)
LA Chg # : Last applied change log no.
Logs TBP : Logs to be transported.
LT Chg # : Last transported change log no.
```

### 4.3.23 The remtool -pilotreplica Operation

The `pilotreplica` operation begins or ends pilot mode for a replica.

### 4.3.23.1 Syntax for remtool -pilotreplica

```
remtool -pilotreplica {begin|end} -bind hostname:ldap_port [-bkup file_name]
```

### 4.3.23.2 Arguments for remtool -pilotreplica

#### **begin | end**

Required. Begin or end pilot mode.

#### **-bind hostname:ldap\_port**

See [Section 4.3.30, "The -bind Connection Argument"](#) for information.

#### **-bkup file\_name**

Name of backup file in which entries modified after pilot mode is started are to be stored in LDIF format.

### 4.3.23.3 Tasks and Examples for remtool -pilotreplica

Using the `pilotreplica` operation you can perform the following tasks:

- [Section 4.3.23.3.1, "Beginning Pilot Mode for a Replica"](#)
- [Section 4.3.23.3.2, "Ending Pilot Mode for a Replica"](#)

#### 4.3.23.3.1 Beginning Pilot Mode for a Replica

##### **Example:**

```
remtool -pilotreplica begin -bind myhost:3060
```

#### 4.3.23.3.2 Ending Pilot Mode for a Replica

##### **Example:**

```
remtool -pilotreplica end -bind myhost:3060
```

## 4.3.24 The remtool -presetpwd Operation

This `presetpwd` operation resets the replication DN password for the given Oracle Internet Directory server in both the directory repository and wallet. It does not reset the passwords for any other directories of the directory replication group (DRG) of which this directory is a member.

You need the Oracle Internet Directory superuser DN and password to reset the replication DN password.

### 4.3.24.1 Syntax for remtool -presetpwd

```
remtool -presetpwd -bind hostname:ldap_port [-v]
```

### 4.3.24.2 Arguments for remtool -presetpwd

You are prompted for the new replication DN password. In addition to the password and arguments supplied on the command-line, the tool prompts you for the following information:

- The superuser DN, for example `cn=orcladmin`.
- The superuser password.

**-bind hostname:ldap\_port**

See [Section 4.3.30, "The -bind Connection Argument"](#) for information.

**4.3.24.3 Tasks and Examples for remtool -presetpwd**

Using the `presetpwd` operation you can perform the following tasks:

- [Section 4.3.24.3.1, "Resetting the Replication DN Password for a Single Directory"](#)

**4.3.24.3.1 Resetting the Replication DN Password for a Single Directory** In this example, the replication DN password is reset for replica `my_host:3040`.

**Example:**

```
remtool -presetpwdd -v -bind my_host:3040
```

The results are:

```
Enter superuser DN                : cn=orcladmin
Enter superuser password          :
-----
Replication DN password of ldap://my_host:3040 (my_host_rem) associated with
database 'rid1' will be reset.
Do you want to continue? [y/n] : y

Enter new password of replication DN :
Reenter new password of replication DN :
-----
ldap://my_host:3040 [my_host_rid1] : Modifying entry cn=replication
dn,orclreplicaid=my_host_rid1,cn=replication configuration...
-----
Password has been changed.
-----
```

**4.3.25 The remtool -pthput Operation**

The `-pthput` option enables you to monitor replication progress in a directory replication group. The tool binds to the specified node and collects information about all the nodes in the directory replication group. It displays this information at intervals of specified duration.

**4.3.25.1 Syntax for remtool -pthput**

```
remtool -pthput [-bind hostname:ldap_port_number] [-interval time_in_seconds]
[-file filename]
```

**4.3.25.2 Arguments for remtool -pthput****-bind hostname:ldap\_port\_number**

See [Section 4.3.30, "The -bind Connection Argument"](#) for information.

**-interval time\_in\_seconds**

The interval for displaying information. This is an optional parameter. Provide its value in seconds. Its default value is 60 seconds.

**-file filename**

The file to write information to. This is an optional argument. If you specify a file argument, the output shown on the command line is logged to that file. Otherwise, the output is logged to a file name based on the timestamp.

**4.3.25.3 Tasks and Examples for remtool -pthput**

Using the `-pthput` option, you can perform the following tasks:

- [Section 4.3.25.3.1, "Listing DRG Information at Intervals"](#)

**4.3.25.3.1 Listing DRG Information at Intervals** In the following example, *time\_in\_seconds* is the value specified by the optional `-interval` parameter.

```
-----
Directory Replication Group (DRG) details :
-----
Sl ReplicaId      Directory Information  Supplier Information  Repl. No.
                                     Type
-----
001 adc2101322_nldap32 adc2101322.us.example.com:3070 adc2101322_nldap3  RW
002 adc2101322_nldap3  adc2101322.us.example.com:3061 adc2101322_nldap32  RW
-----
Queue Statistics :
Interval for refreshing stats is time_in_seconds seconds.
-----
-----
Supplier          Consumer          Queued          Last Applied          Applied
Average
                                     Changes          Change Number          Changes
Throughput
Of 3 intervals
-----
-----
adc2101322_nldap3  adc2101322_nldap32  0          134369          0
0
adc2101322_nldap32  adc2101322_nldap3  0          47342          0
0
-----
-----
adc2101322_nldap3  adc2101322_nldap32  2286          136214          1845
615
adc2101322_nldap32  adc2101322_nldap3  0          47342          0
0
-----
-----
adc2101322_nldap3  adc2101322_nldap32  1608          137886          1672
1172
adc2101322_nldap32  adc2101322_nldap3  0          47342          0
0
-----
-----
adc2101322_nldap3  adc2101322_nldap32  189          140302          2416
1977
adc2101322_nldap32  adc2101322_nldap3  0          47342          0
0
-----
-----
```

## 4.3.26 The remtool -pverify Operation

The `pverify` operation verifies the replication configuration for a directory replication group (DRG) that uses LDAP-based replication. This operation cannot be used for a DRG that uses ASR based replication. If a DRG uses both ASR and LDAP-based replication, then this option verifies the replication configuration between nodes that use LDAP-based replication only.

The `pverify` operation has the following usage rules:

- This option only verifies agreements that involve the node specified in the command argument.
- The `remtool_VERIFY_LOG.rpt` report contains the verification results.

### 4.3.26.1 Syntax for remtool -pverify

```
remtool -pverify [-bind hostname:ldap_port_number] [-hiqmax hiqmax] [-tbtmax
tbtmax] [-v]
```

### 4.3.26.2 Arguments for remtool -pverify

#### **-bind hostname:ldap\_port\_number**

See [Section 4.3.30, "The -bind Connection Argument"](#) for information.

#### **-hiqmax hiqmax**

The maximum number of change logs in the Human Intervention Queue (HIQ) after which warnings are generated.

#### **-tbtmax tbtmax**

The maximum number of logs to be transported (tbt) after which warnings are generated.

### 4.3.26.3 Tasks and Examples for remtool -pverify

Use the `pverify` operation to perform the following tasks:

- [Section 4.3.26.3.1, "Verify Replication Configuration for an LDAP-Based DRG"](#)

**4.3.26.3.1 Verify Replication Configuration for an LDAP-Based DRG** In this example, the replication configuration for a DRG comprising of directory servers `ldap://my_host:3040`, `ldap://my_host:3060`, and `ldap://my_host:3080` is verified.

#### **Example**

```
remtool -pverify -v -bind my_host:3040
```

```
Node ID: my_host_rid1 Test Category: Connection
Test Against: my_host_rid1
Test: Wallet
Check: Corruption passed
Check: Authentication passed
Check: Replicationdn passed

Test Against: my_host_rid2
Test: URL
Check: Format (Primary) passed
```

Check: Format (Secondary) passed

Test Against: my\_host\_rid3  
Test: URL  
Check: Format (Primary) passed  
Check: Format (Secondary) passed

Test Against: my\_host\_rid1  
Test: URL  
Check: Format (Primary) passed  
Check: Format (Secondary) passed

Test Category: Agreements  
Test Against: Agrmt 000002  
Test: orclreplicadn  
Check: Validity passed  
Check: Match agreement type passed

Test: agreement DN  
Check: Format passed

Test Against: Agrmt 000002 with my\_host\_rid2  
Test: lastAppliedChangeNumber (my\_host\_rid2 to my\_host\_rid1)  
Check: Format (transport) passed  
Check: Logs TBP passed  
Check: Format (apply) passed  
Check: HIQ passed

Test: Filtering (my\_host\_rid2 to my\_host\_rid1)  
Check: Format passed  
Check: Configuration passed

Test Against: Agrmt 000002 with my\_host\_rid2  
Test: Connection  
Check: Authentication passed

Test: Replica Pair  
Check: Validity passed  
Check: Consistency passed

Test: orclreplicationid  
Check: Availability passed

Test: Replication Protocol  
Check: Availability passed

Test: lastAppliedChangeNumber (my\_host\_rid1 to my\_host\_rid2)  
Check: Format (transport) passed  
Check: Logs TBP passed  
Check: Format (apply) passed  
Check: HIQ passed

Test: Filtering (my\_host\_rid1 to my\_host\_rid2)  
Check: Format passed  
Check: Configuration passed

Test Against: Agrmt 000003  
Test: orclreplicadn  
Check: Validity passed  
Check: Match agreement type passed

```

Test: agreement DN
      Check: Format passed

Test Against: Agrmt 000003 with my_host_rid3
Test: lastAppliedChangeNumber (my_host_rid3 to my_host_rid1)
      Check: Format (transport) passed
      Check: Logs TBP passed
      Check: Format (apply) passed
      Check: HIQ passed

Test: Filtering (my_host_rid3 to my_host_rid1)
      Check: Format passed
      Check: Configuration failed

Test Against: Agrmt 000003 with my_host_rid3
Test: Connection
      Check: Authentication passed

Test: Replica Pair
      Check: Validity passed
      Check: Consistency passed

Test: orclreplicationid
      Check: Availability passed

Test: Replication Protocol
      Check: Availability passed

Test: lastAppliedChangeNumber (my_host_rid1 to my_host_rid3)
      Check: Format (transport) passed
      Check: Logs TBP passed
      Check: Format (apply) passed
      Check: HIQ passed

Test: Filtering (my_host_rid1 to my_host_rid3)
      Check: Format passed
      Check: Configuration failed

Verify replication configuration for my_host_rid1 successfully.

Refer to remtool_VERIFY_LOG.rpt for details.

2 checks failed.

```

## 4.3.27 The remtool -resumeasr Operation

The `resumeasr` operation resumes replication activity for an Oracle Database Advanced Replication-based directory replication group (DRG) that was previously suspended using the [Section 4.3.28, "The remtool -suspendasr Operation."](#)

### 4.3.27.1 Syntax for remtool -resumeasr

```
remtool -resumeasr [-connect repl_admin_name@net_service_name] [-v]
```

### 4.3.27.2 Arguments for remtool -resumeasr

#### -connect repl\_admin\_name@net\_service\_name

For more information, see [Section 4.3.31, "The -connect Connection Argument."](#)

### 4.3.27.3 Tasks and Examples for remtool -resumeasr

Using the resumeasr operation you can perform the following tasks:

- [Section 4.3.27.3.1, "Resuming Replication Activity for an Advanced Replication-Based DRG"](#)

**4.3.27.3.1 Resuming Replication Activity for an Advanced Replication-Based DRG** In this example, replication activity of DRG consisting of MY\_HOST1.MY\_COMPANY.COM and MY\_HOST2.MY\_COMPANY.COM is resumed.

#### Example:

```
remtool -resumeasr -v -conn repadmin@MY_HOST1.MY_COMPANY.COM
```

The results are:

```
MY_HOST1.MY_COMPANY.COM is Master Definition Site (MDS). Connected to MDS.
```

```
MY_HOST2.MY_COMPANY.COM is Remote Master Site (RMS). Connected to RMS.
```

```
Directory Replication Group (DRG) details :
```

```
-----
Instance Host Name      Global Name              Version      Replicaid      Site
Name                                     Type
-----
rid1      my_host      MY_HOST1.MY_COMPANY.COM  OID 9.0.4.0.0  my_host_rid1  MDS
rid2      my_host      MY_HOST2.MY_COMPANY.COM  OID 9.0.4.0.0  my_host_rid2  RMS
-----
```

```
Altering replication status...
```

```
MY_HOST1.MY_COMPANY.COM : Resuming replication activity...
```

```
-----
Replication status has been altered successfully.
-----
```

## 4.3.28 The remtool -suspendasr Operation

The suspendasr operation suspends Oracle Database Advanced Replication activity for a directory replication group (DRG) that uses it for replication. While Advanced Replication activity is suspended, replication does not take place.

### 4.3.28.1 Syntax for remtool -suspendasr

```
remtool -suspendasr [-connect repl_admin_name@net_service_name] [-v]
```

### 4.3.28.2 Arguments for remtool -suspendasr

#### -connect repl\_admin\_name@net\_service\_name

The connection string for the master definition site (MDS) or the Remote Master Site (RMS). You are prompted for the password for the replication administrator. If you do not supply an argument on the command-line, the tool prompts you for the information. The connect string is composed of the following elements:

- The name of the replication administrator.



- The net service name of the MDS or RMS. If you have a `tnsnames.ora` file configured, then this is the net service name specified in that file, which is located by default in `ORACLE_INSTANCE/config`. (You can set the `TNS_ADMIN` environment variable if you want to use a different location.)

### 4.3.28.3 Tasks and Examples for `remtool -suspendasr`

Using the `suspendasr` operation you can perform the following tasks:

- [Section 4.3.28.3.1, "Suspending Replication Activity for an Advanced Replication-Based DRG"](#)

**4.3.28.3.1 Suspending Replication Activity for an Advanced Replication-Based DRG** In this example, replication activity of a DRG consisting of `MY_HOST1.MY_COMPANY.COM` and `MY_HOST2.MY_COMPANY.COM` is suspended.

#### Example:

```
remtool -suspendasr -v -conn repadmin@my_host1.my_company.com
```

The results are:

```
MY_HOST1.MY_COMPANY.COM is Master Definition Site (MDS). Connected to MDS.
MY_HOST2.MY_COMPANY.COM is Remote Master Site (RMS). Connected to RMS.
Directory Replication Group (DRG) details :
```

```
-----
Instance Host Name      Global Name              Version      ReplicaId      Site
Name                                                    Type
-----
rid      my_host      MY_HOST1.MY_COMPANY.COM 10.1.2.0.0  my_host_rid1  MDS
rid2     my_host      MY_HOST2.MY_COMPANY.COM 10.1.2.0.0  my_host_rid2  RMS
-----
```

```
Altering replication status...
```

```
MY_HOST1.MY_COMPANY.COM : Quiescing replication activity...
```

```
-----
Replication status has been altered successfully.
-----
```

## 4.3.29 The `-psuspendrepl` and `-presumerepl` Operations

The `-psuspendrepl` and `-presumerepl` operations provide rolling upgrade support for multimaster replication DRGs by suspending and resuming replication, respectively.

### 4.3.29.1 Syntax for `-psuspendrepl` and `-presumerepl`

```
remtool -psuspendrepl -fromnode host1:port1 [-tonode host2:port2]
```

```
remtool -presumerepl -fromnode host1:port1 [-tonode host2:port2]
```

---

**Note:** You must apply all required patches before starting the rolling upgrade procedure.

---

### 4.3.29.2 Arguments to `-psuspendrepl` and `-presumerepl`

#### `-fromnode host1:port1`

Specifies the host and port of the node from which replication is to be suspended.

#### `-tonode host2:port2`

Specifies the host and port of the node to which replication is to be suspended

If you do not specify the `-tonode` parameter with `-psuspendrepl` or `-presumerepl`, `remtool` displays the replicaids of all the replicas and prompts you for the replica to which to replication is to be suspended or resumed. To suspend or resume replication to all the replicas, enter `all`.

For example:

```
remtool -psuspendrepl -fromnode :5060/ods
```

```
-----
Directory Replication Group (DRG) details :
```

Sl Version. No.	Replicaid	Directory Information	Supplier Information	Repl Type	OID
001	adc2101322_gps3	adc2101322:3060	adc2170827_sldap2	RW	111140
002	adc2170827_sldap2	adc2170827:3070	adc2101322_gps3	RW	111140

```
-----
Enter replicaid of the replica to be suspended[Enter "all" to select all
replicas]:
```

### 4.3.29.3 Tasks for `-psuspendrepl` and `-presumerepl`

The procedure for rolling upgrade can be summarized as follows:

1. Stop the replication server on the replica to be upgraded.
2. Run `remtool -psuspendrepl`.
3. Stop Oracle Internet Directory on the replica to be upgraded.
4. Upgrade the replica.
5. Start Oracle Internet Directory on the upgraded replica.
6. Run `remtool -presumerepl`.
7. Start the replication server on the upgraded replica.

**See Also:** The appendix "Performing a Rolling Upgrade" in *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory* for more details and an example of rolling upgrade.

## 4.3.30 The `-bind` Connection Argument

This argument is used with LDAP-based operations to supply the host and port of the supplier. The syntax is:

```
bind supplier_hostname:ldap_port
```

You are prompted for the replication DN password. If you omit either the hostname or port or both, `remtool` uses the local host name or default port (3060) or both as arguments. If you omit the `-bind` argument, you are prompted for the missing information.

### 4.3.31 The `-connect` Connection Argument

This argument is used with Oracle Database Advanced Replication-based operations to specify connection string for the master definition site (MDS) or the Remote Master Site (RMS). The syntax is:

```
-connectrepl_admin_name@net_service_name
```

You are prompted for the replication DN password. If you do not supply an argument on the command-line, the tool prompts you for the information.

### 4.3.32 Related Command-Line Tools for `remtool`

- See "`oidctl`" on page 2-4
- See "`opmnctl`" on page 2-15



---

# Oracle Directory Integration Platform Tools

This chapter describes the command-line tools used to administer Oracle Directory Integration Platform.

This chapter includes the following sections:

- Section 5.1, "manageDIPServerConfig"
- Section 5.2, "manageSyncProfiles"
- Section 5.3, "syncProfileBootstrap"
- Section 5.4, "expressSyncSetup"
- Section 5.5, "provProfileBulkProv"
- Section 5.6, "oidprovtool" (Provisioning Registration Tool)
- Section 5.7, "dipStatus"
- Section 5.8, "schemasync"

---

## Notes:

- Best security practice is to provide a password only in response to a prompt from the command.
  - You must set the environment variables `WLS_HOME` and `ORACLE_HOME` before executing any of the Oracle Directory Integration Platform commands.
  - The Oracle WebLogic Managed Server where Oracle Directory Integration Platform is deployed must be configured for SSL to execute the Oracle Directory Integration Platform commands in SSL mode. Refer to the *Configuring SSL* chapter in *Oracle Fusion Middleware Securing Oracle WebLogic Server* for more information.
- 

## 5.1 manageDIPServerConfig

The Manage DIP Server Configuration utility, `manageDIPServerConfig`, allows you to manage the Oracle Directory Integration Platform server configuration.

### 5.1.1 Syntax for manageDIPServerConfig

#### **manageDIPServerConfig**

```
manageDIPServerConfig {get | set} -h HOST -p PORT -D wlsuser -attribute {sslmode |  
refreshinterval | quartzthreadcount | quartzdbretryinterval | oidhostport |
```

```
keystorelocation} [-ssl -keystorePath PATH_TO_KEYSTORE -keystoreType TYPE]
[-value ATTRIBUTE_VALUE] [-help]
```

## 5.1.2 Arguments for manageDIPServerConfig

### **get | set**

Operation to perform.

- **get**: Displays the current value of the config parameter in DIP configuration file
- **set**: Updates the value of the config parameter in DIP configuration file.

### **-h | -host**

Oracle WebLogic Server host where Oracle Directory Integration Platform is deployed

### **-p | -port**

Listen port of Oracle WebLogic Managed Server where Oracle Directory Integration Platform application is deployed.

### **-D | -wlsuser**

WebLogic Server login ID.

---

---

**Note:** You are prompted for the Oracle WebLogic Server login password. You cannot provide the password as a command-line argument. Best security practice is to provide a password only in response to a prompt from the command. If you must execute `manageDIPServerConfig` from a script, you can redirect input from a file containing the Oracle WebLogic Server login password. Use file permissions to protect the file and delete it when it is no longer necessary.

---

---

### **-attr | -attribute**

Identifies the attribute that `manageDIPServerConfig` performs the operation on. The following is a list and description of the attributes `manageDIPServerConfig` can perform operations on:

- **sslmode**: The SSL mode Oracle Directory Integration Platform uses to connect to Oracle Internet Directory. Supported values are 1 and 2. Use 1 to connect to Oracle Internet Directory using SSL Mode 1 (No Authentication). Use 2 to connect to Oracle Internet Directory using SSL Mode 2 (Server Only Authentication).
- **refreshinterval**: The time interval (amount of time in seconds) that controls how often the Oracle Directory Integration Platform server refreshes profile configuration details.
- **quartzthreadcount**: Controls how many profiles can be scheduled in parallel. The default value is 15. If you have more than 15 profiles, increase the `quartzthreadcount` attribute accordingly.
- **quartzdbretryinterval**: Controls how often Oracle Directory Integration Platform's Quartz scheduler attempts to reconnect to the Oracle Internet Directory database.

- `oidhostport`: Identifies the host and port of the Oracle Internet Directory associated with Oracle Directory Integration Platform. Specify values for the `oidhostport` attribute in the form of `host:port`.
- `keystorelocation`: Specifies the absolute path to the Java Keystore (JKS) based on the host where Oracle Directory Integration Platform is deployed. When you specify the value for the `keystorelocation` attribute, be sure you use the appropriate path separators (that is, `/` for UNIX and Linux platforms, and `\` for Windows platforms).

**-ssl**

Executes the command in SSL mode.

---



---

**Note:** The Oracle WebLogic Managed Server where Oracle Directory Integration Platform is deployed must be configured for SSL to execute this command in SSL mode. Refer to the *Configuring SSL* chapter in *Oracle Fusion Middleware Securing Oracle WebLogic Server* for more information.

---



---

**-keystorePath**

The full path to the keystore.

**-keystoreType**

The type of the keystore identified by `-keystorePath`. For example: `-keystorePath jks` or `-keystorePath PKCS12`

**-val | -value**

The value to set for the attribute This parameter is required with the set operation.

**-help**

Provides usage help for the command.

### 5.1.3 Tasks and Examples for manageDIPServerConfig

```
manageDIPServerConfig get -h myhost.mycompany.com -p 7005 -D weblogic \
  -attr sslmode
```

```
manageDIPServerConfig set -h myhost.mycompany.com -p 7005 -D weblogic \
  -attr sslmode -val 2
```

## 5.2 manageSyncProfiles

The Manage Synchronization Profiles utility, `manageSyncProfiles`, allows you to manage synchronization profiles.

### 5.2.1 Syntax for manageSyncProfiles

**managSyncProfiles**

```
manageSyncProfiles {activate | deactivate | copy | deregister | get | isexists |
  update | testProfile | validateProfile | validateMapRules | register |
  updatechgnum | associateProfile | dissociateProfile | getAllAssociatedProfiles |
```

```
getAssociatedProfile | list } -h HOST -p PORT -D wlsuser [-ssl -keystorePath
PATH_TO_KEYSTORE -keystoreType TYPE] [-profile] [-newProfile]
[-associateProfile][-file] [-params 'prop1 val1 prop2 val2 ...']
[-conDirHost] [-conDirPort] [-conDirBindDn] [-mode] [-conDirType] [-conDirSSL]
[-profileStatus] [-help]
```

## 5.2.2 Arguments for manageSyncProfiles

### Operations

#### **activate**

Changes a profile state to ENABLE

#### **deactivate**

Changes a profile state to DISABLE

#### **copy**

Copies an existing profile to profile *newProfile*

#### **deregister**

Deletes an existing profile from OID.

#### **get**

Gets the profile details from OID.

#### **isexists**

Checks if the profile *profile* exists in OID.

#### **update**

Modifies an existing profile *profile* in OID.

#### **testProfile**

Changes the state of a disabled profile *profile* to TEST and schedules the profile for testing to ensure the profile successfully performs synchronization. After executing the manageSyncProfiles command with the testProfile operation, the results of the test are available in the following log file, where *DOMAIN\_HOME* represents the Oracle WebLogic Server Domain home and *ORACLE\_WEBLOGIC\_MANAGED\_SERVER\_NAME* represents the name of the managed server where Oracle Directory Integration Platform is deployed:

```
DOMAIN_HOME/servers/ORACLE_WEBLOGIC_MANAGED_SERVER_NAME/logs/ORACLE_WEBLOGIC_MANAGED_SERVER_NAME.log
```

---

---

**Note:** The testProfile operation cannot schedule profiles that are in ENABLE state for testing.

---

---

#### **validateProfile**

Validates the syntax of the values in the specified profile for correctness.



**validateMapRules**

Validates the map rules provided.

**register**

Creates a new profile in OID.

**updatechgnum**

Updates the last applied change number in the profile to latest.

**associateProfile**

Associates *associateProfileName* with *profileName* to prevent information back flow.

**dissociateProfile**

Dissociates an associated profile to *profileName*

**getAllAssociatedProfiles**

Lists all the profiles to which profile *profileName* is associated.

**getAssociatedProfile**

Displays the profile name associated with profile *profileName*.

**list**

Displays all profiles registered in OID.

**Options****-h | host**

Oracle WebLogic Server host where Oracle Directory Integration Platform is deployed.

**-p | -port**

Listen port of Oracle WebLogic Managed Server where Oracle Directory Integration Platform application is deployed.

**-D | wlsuser**

Oracle WebLogic Server login ID

---

---

**Note:** You are prompted for the Oracle WebLogic Server login password. You cannot provide the password as a command-line argument. Best security practice is to provide a password only in response to a prompt from the command. If you must execute a command from a script, you can redirect input from a file containing the Oracle WebLogic Server login password. Use file permissions to protect the file and delete it when it is no longer necessary. If you must provide more than one password to `manageSyncProfiles`, put each on a separate line in the file, in the following order: connected directory bind DN password, then Oracle WebLogic Server login password.

---

---

**-ssl**

Executes the command in SSL mode.

---

---

**Note:** The Oracle WebLogic Managed Server where Oracle Directory Integration Platform is deployed must be configured for SSL to execute this command in SSL mode. Refer to the *Configuring SSL* chapter in *Oracle Fusion Middleware Securing Oracle WebLogic Server* for more information.

---

---

**-keystorePath**

The full path to the keystore.

**-keystoreType**

The type of the keystore identified by `-keystorePath`. For example: `-keystorePath jks` or `-keystorePath PKCS12`

**-pf | -profile**

The name of the synchronization profile to use when performing the operation.

**-newpf | -newProfile**

The name of the new profile which will be a copy of *profile*.

**-assopf**

The name of the profile that will be associated with *profile*

**-f | -file**

The full path and file name of the profile properties file containing the properties. See the "Example Properties File for Synchronization Profiles" appendix in *Oracle Fusion Middleware Administrator's Guide for Oracle Directory Integration Platform* for an example of such a file.

**-params**

A value is of the form `prop1 val1 prop2 val2 ...` where `prop` is the name of a profile property and `val` is the new value for that property. This keyword is used only for modification of a profile. You can specify as many key values as required

**-conDirHost**

Host where connected directory server is running.

**-conDirPort**

Port at which connected directory server listens.

**-conDirBindDn**

Connected directory server bind DN.

Examples:

- Active Directory  
administrator@idm2003.net
- Sun ONE or iPlanet  
cn=Directory Manager
- Oracle Internet Directory

```
cn=orcladmin
```

---



---

**Note:** You are prompted for the connected directory bind DN password. You cannot provide the password as a command-line argument. Best security practice is to provide a password only in response to a prompt from the command. If you must execute `manageSyncProfiles` from a script, you can redirect input from a file containing the connected directory bind DN password. Use file permissions to protect the file and delete it when it is no longer necessary. If you must provide more than one password to `manageSyncProfiles`, put each on a separate line in the file, in the following order: connected directory bind DN password, then Oracle WebLogic Server login password.

---



---

**-mode**

Synchronization mode map rules to be used: import or export

**-conDirType**

Connected directory type. Supported values are ActiveDirectory, EDirectory, iPlanet, OpenLDAP, ADAM, Tivoli, ExchangeServer2003, and OID.

**-conDirSSL**

SSL mode value used to connect connected directory server

**-prfSt | -profileStatus**

Displays status for the profile. Used only with the list operation.

**-help**

Provides command usage help.

## 5.2.3 Tasks and Examples for manageSyncProfiles

```
manageSyncProfiles register -h myhost.mycompany.com -p 7005 -D weblogic \
  -f /opt/ldap/odip/iPlImport.profile
```

```
manageSyncProfiles deregister -h myhost.mycompany.com -p 7005 \
  -D weblogic -pf myProfile
```

```
manageSyncProfiles updatechgnum -h myhost.mycompany.com -p 7005 \
  -D weblogic -pf myProfile
```

```
manageSyncProfiles activate -h myhost.mycompany.com -p 7005 \
  -D weblogic -pf myProfile
```

```
manageSyncProfiles deactivate -h myhost.mycompany.com -p 7005 \
  -D weblogic -pf myProfile
```

```
manageSyncProfiles get -h myhost.mycompany.com -p 7005 \
  -D weblogic -pf myProfile
```

```
manageSyncProfiles testProfile -h myhost.mycompany.com -p 7005 \
  -D weblogic -pf myProfile
```

```
manageSyncProfiles associateprofile -h myhost.mycompany.com -p 7005 \  
-D weblogic -pf myProfile -assopf myProfile1  
  
manageSyncProfiles dissociateprofile -h myhost.mycompany.com -p 7005 \  
-D weblogic -pf myProfile  
  
manageSyncProfiles getAllAssociatedProfiles -h myhost.mycompany.com -p 7005 \  
-D weblogic -pf myProfile  
  
manageSyncProfiles getAssociatedProfile -h myhost.mycompany.com -p 7005 \  
-D weblogic -pf myProfile  
  
manageSyncProfiles update -h myhost.mycompany.com -p 7005 \  
-D weblogic -pf myProfile -f /opt/ldap/odip/iPlImport.profile  
  
manageSyncProfiles validateMapRules -h myhost.mycompany.com -p 7005 \  
-D weblogic -f /opt/ldap/odip/iPlImport.map -conDirHost server.example.com \  
-conDirPort 8000 -conDirBindDn administrator@idm2003.net -mode IMPORT \  
-conDirType IPLANET  
  
manageSyncProfiles isexists -h myhost.mycompany.com -p 7005 -D weblogic \  
-pf myProfile  
  
manageSyncProfiles copy -h myhost.mycompany.com -p 7005 -D weblogic \  
-pf myProfile -newpf yourProfile  
  
manageSyncProfiles list -h myhost.mycompany.com -p 7005 -D weblogic -profileStatus
```

## 5.3 syncProfileBootstrap

The Synchronization Profile Bootstrap utility, `syncProfileBootstrap`, performs the initial migration of data between a connected directory and Oracle Internet Directory for a synchronization profile.

### 5.3.1 Syntax for syncProfileBootstrap

#### **syncProfileBootstrap**

```
syncProfileBootstrap -h HOST -p PORT -D wlsuser {-file FILENAME | -profile  
-PROFILE_NAME} [-ssl -keystorePath PATH_TO_KEYSTORE -keystoreType TYPE]  
[-loadParallelism INTEGER] [-loadRetry INTEGER] [-help]
```

### 5.3.2 Arguments for syncProfileBootstrap

#### **-h | -host**

Oracle WebLogic Server host where Oracle Directory Integration Platform is deployed.

#### **-p | -port**

Listen port of Oracle WebLogic Managed Server where Oracle Directory Integration Platform application is deployed.

#### **-D | wlsuser**

Oracle WebLogic Server login ID

---



---

**Note:** You are prompted for the Oracle WebLogic Server login password. You cannot provide the password as a command-line argument. Best security practice is to provide a password only in response to a prompt from the command. If you must execute `syncProfileBootstrap` from a script, you can redirect input from a file containing the Oracle WebLogic Server login password. Use file permissions to protect the file and delete it when it is no longer necessary.

---



---

**-f | -file**

Bootstrap properties file.

**-pf | -profile**

The name of the synchronization profile to use when performing the operation.

**-ssl**

Executes the command in SSL mode.

---



---

**Note:** The Oracle WebLogic Managed Server where Oracle Directory Integration Platform is deployed must be configured for SSL to execute this command in SSL mode. Refer to the *Configuring SSL* chapter in *Oracle Fusion Middleware Securing Oracle WebLogic Server* for more information.

---



---

**-keystorePath**

The full path to the keystore.

**-keystoreType**

The type of the keystore identified by `-keystorePath`. For example: `-keystorePath jks` or `-keystorePath PKCS12`

**-lp | -loadParallelism**

Indicator that loading to Oracle Internet Directory is to take place in parallel by using multiple threads. For example, `-loadparallelism 5` means that 5 threads are to be created, each of which tries to load the entries in parallel to Oracle Internet Directory.

**-lr | -loadRetry**

The number of times the retry should be made (when the load to the destination fails) before marking the entry as bad entry.

**-help**

Provides command usage help.

### 5.3.3 Tasks and Examples for syncProfileBootstrap

```
manageSyncProfileBootstrap -h myhost.mycompany.com -p 7005 -D weblogic \
  -pf myProfile -lp 5
```

```
manageSyncProfileBootstrap -h myhost.mycompany.com -p 7005 -D weblogic \
  -f /opt/ldap/odip/bootstrap.properties -lr 3
```

## 5.4 expressSyncSetup

The Express Synchronization Setup utility, `expressSyncSetup`, creates import and export synchronizations profiles.

### 5.4.1 Syntax for expressSyncSetup

#### **expressSyncSetup**

```
expressSyncSetup -h HOST -p PORT -D wlsuser -pf PROFILE
-conDirType CONNECTED_DIRECTORY_TYPE -conDirURL CONNECTED_DIRECTORY_URL
-conDirBindDN CONNECTED_DIRECTORY_BIND_DN -conDircontainer SYNC_CONTAINER
[-ssl -keystorePath PATH_TO_KEYSTORE -keystoreType TYPE] [-enableProfiles {true |
false}] [-help]
```

### 5.4.2 Arguments for expressSyncSetup

#### **-h | -host**

Oracle WebLogic Server host where Oracle Directory Integration Platform is deployed.

#### **-p | -port**

Listen port of Oracle WebLogic Managed Server where Oracle Directory Integration Platform application is deployed.

#### **-D | wlsusser**

Oracle WebLogic Server login ID

---

---

**Note:** You are prompted for the Oracle WebLogic Server login password. You cannot provide the password as a command-line argument. Best security practice is to provide a password only in response to a prompt from the command. If you must execute `expressSyncSetup` from a script, you can redirect input from a file containing the Oracle WebLogic Server login password. Use file permissions to protect the file and delete it when it is no longer necessary. If you must provide more than one password to `expressSyncSetup`, put each on a separate line in the file, in the following order: connected directory bind DN password, then Oracle WebLogic Server login password.

---

---

#### **-pf | -profile**

Profile name.

#### **-conDirType**

Connected directory type. Supported values are `ActiveDirectory`, `EDirectory`, `iPlanet`, `OpenLDAP`, `ADAM`, `Tivoli`, `ExchangeServer2003`, and `OID`.

#### **-conDirUrl**

URL where the connected directory is running. The format is *host:port*.

#### **-conDirBindDN**

Connected directory server bind DN. For example:

```
administrator@idm2003.net
cn=orcladmin,cn=Directory Manager
```

---



---

**Note:** You are prompted for the connected directory bind DN password. You cannot provide the password as a command-line argument. Best security practice is to provide a password only in response to a prompt from the command. If you must execute `expressSyncSetup` from a script, you can redirect input from a file containing the connected directory bind DN password. Use file permissions to protect the file and delete it when it is no longer necessary. If you must provide more than one password to `expressSyncSetup`, put each on a separate line in the file, in the following order: connected directory bind DN password, then Oracle WebLogic Server login password.

---



---

#### **-conDirContainer**

The synchronization container. For example:

```
ou=sales,dc=us,dc=com
OU=Groups,DC=imtest,DC=com
CN=Users,DC=imtest,DC=com
```

#### **-ssl**

Executes the command in SSL mode.

---



---

**Note:** The Oracle WebLogic Managed Server where Oracle Directory Integration Platform is deployed must be configured for SSL to execute this command in SSL mode. Refer to the *Configuring SSL* chapter in *Oracle Fusion Middleware Securing Oracle WebLogic Server* for more information.

---



---

#### **-keystorePath**

The full path to the keystore.

#### **-keystoreType**

The type of the keystore identified by `-keystorePath`. For example: `-keystorePath jks` or `-keystorePath PKCS12`

#### **-enableProfiles**

Specify `true` to enable created profiles, `false` if not.

#### **-help**

Provides command usage help.

### 5.4.3 Tasks and Examples for `expressSyncSetup`

```
expressSyncSetup -h myhost.mycompany.com -p 7005 -D weblogic -pf myProfile \  
-conDirType ACTIVE DIRECTORY -conDirUrl server.mycompany.com:5432 \  
-conDirBindDN administrator@idm2003.net -conDirContainer ou=sales,dc=us,dc=com \  
-enableProfiles false \  

```

```
expressSyncSetup -help
```

## 5.5 provProfileBulkProv

The Provisioning Profile Bulk utility, `provProfileBulkProv`, performs initial migration of data from an LDIF file to Oracle Internet Directory for a provisioning profile.

### 5.5.1 Syntax for provProfileBulkProv

#### **provProfileBulkProv**

```
provProfileBulkProv -h HOST -p PORT -D wlsuser -file LDIF_FILE -realm REALM_DN  
[-ssl -keystorePath PATH_TO_KEYSTORE -keystoreType TYPE]  
[-encoding INPUT_ENCODING] [-help]
```

### 5.5.2 Arguments for provProfileBulkProv

#### **-h | -host**

Oracle WebLogic Server host where Oracle Directory Integration Platform is deployed.

#### **-p | -port**

Listen port of Oracle WebLogic Managed Server where Oracle Directory Integration Platform application is deployed.

#### **-D | -wlsuser**

Oracle WebLogic Server login ID

---

---

**Note:** You are prompted for the Oracle WebLogic Server login password. You cannot provide the password as a command-line argument. Best security practice is to provide a password only in response to a prompt from the command. If you must execute `provProfileBulkProv` from a script, you can redirect input from a file containing the Oracle WebLogic Server login password. Use file permissions to protect the file and delete it when it is no longer necessary.

---

---

#### **-f | -file**

LDIF file containing the data to be migrated.

#### **-realm**

The realm in which the users are to be provisioned.

#### **-ssl**

Executes the command in SSL mode.



---



---

**Note:** The Oracle WebLogic Managed Server where Oracle Directory Integration Platform is deployed must be configured for SSL to execute this command in SSL mode. Refer to the *Configuring SSL* chapter in *Oracle Fusion Middleware Securing Oracle WebLogic Server* for more information.

---



---

**-keystorePath**

The full path to the keystore.

**-keystoreType**

The type of the keystore identified by `-keystorePath`. For example: `-keystorePath jks` or `-keystorePath PKCS12`

**-encoding**

Input file encoding.

**-help**

Provides command usage help.

### 5.5.3 Tasks and Examples for provProfileBulkProv

```
provProfileBulkprov -h myhost.mycompany.com -p 7005 -D weblogic \
-f /opt/ldap/odip/users.ldif -realm cn=aaaa,ou=bbbb,dc=cccc
```

## 5.6 oidprovtool

Provisioning enables you to ensure that an application is notified of directory changes, such as changes to user or group information. Such changes can affect whether the application allows a user access to its processes and resources.

When you install an application that you want to provision, you must create a provisioning integration profile by using the Provisioning Registration Tool (`oidprovtool`).

You can use the Provisioning Registration Tool to:

- Create a new provisioning profile. A new provisioning profile is created and set to the enabled state so that Oracle Directory Integration Platform can process it.
- Disable an existing provisioning profile.
- Enable a disabled provisioning profile.
- Modify an existing provisioning profile.
- Delete an existing provisioning profile.
- Get the current status of a given provisioning profile.
- Clear all of the errors in an existing provisioning profile.

The Provisioning Registration Tool shields the location and schema details of the provisioning profile entries from the callers of the tool. From the callers' perspective, the combination of an application and a realm uniquely identify a provisioning profile. The constraint in the system is that there can be only one provisioning profile for each application for each realm.

Once a profile is created, its mode—that is, INBOUND, OUTBOUND, or BOTH—cannot be changed by using the `modify` operation. To change the mode, you must delete, then re-create, the profile.

The Oracle directory integration platform server automatically monitors provisioning profile configuration changes in Oracle Internet Directory, including the creation, modification, and deletion of provisioning profiles. For this reason, you do not need to manually enable or disable a provisioning profile.

---



---

**Note:** For improved security, do not supply a password on the command line. The `oidprovtool` command prompts you for a password if you do not supply one on the command line.

---



---

## 5.6.1 Syntax for oidprovtool

### oidprovtool

```
oidprovtool operation=[create|modify] ldap_host=oid_hostname ldap_port=port
ldap_user_dn="bindDN" ldap_user_password=password
[profile_mode=INBOUND|OUTBOUND|BOTH]
application_dn="DN" application_type=type [application_name=name]
[application_display_name=display name] organization_dn=DN
[application_isdasvisible=TRUE|FALSE] [manage_application_defaults=TRUE|FALSE]
[enable_bootstrap=TRUE|FALSE] [user_data_location=DN]
[default_provisioning_policy=PROVISIONING_REQUIRED|PROVISIONING_NOT_REQUIRED]
interface_name=SCHEMA.PACKAGE [interface_type=PLSQL|JAVA]
interface_version=1.1|2.0|3.0 interface_connect_info=connection_string
schedule=number_seconds lastchangenumber=number
max_prov_failure_limit=number
max_events_per_schedule=number max_events_per_invocation=number
event_mapping_rules="OBJECT_TYPE:FILTER:DOMAIN"
event_permitted_operations="OBJECT:DOMAIN:OPERATION(attributes,...)"
event_subscription="USER|GROUP:DOMAIN:OPERATION(attributes,...)"
max_events_per_schedule=number max_retries=number profile_group=number
profile_status=ENABLED | DISABLED profile_debug=debug_level

oidprovtool {operation=enable|disable|delete|status|reset}
application_dn=DN [organization_dn=DN] [ldap_host=oid_hostname] [ldap_port=port]
[ldap_user_dn=bindDN] [ldap_user_password=password] [profile_debug=debug_level]
```

## 5.6.2 Arguments for oidprovtool

### operation=create | modify | enable | disable | delete | status | reset

Required. The operation to perform using `oidprovtool`. You can only perform one operation at a time. The operations are:

- `create`—Creates a new provisioning profile.
- `modify`—Modifies the given properties of an existing provisioning profile.
- `enable`—Enables a provisioning profile.
- `disable`—Disables a provisioning profile.
- `delete`—Deletes a provisioning profile.
- `status`—Shows the current status of a given provisioning profile.
- `reset`—Clears all errors for a provisioning profile.

**ldap\_host=oid\_hostname**

Optional. The host name of the Oracle Internet Directory server. If not provided then the name of the local host is used.

**ldap\_port=port**

Optional. The LDAP listening port of Oracle Internet Directory. The default is 3060.

**ldap\_user\_dn=bindDN**

Required. The DN of the superuser or a user that has sufficient permissions to perform provisioning subscription operations. The default is `cn=orcladmin`.

**ldap\_user\_password=password**

Optional. The user password used to bind to the directory. If you do not specify the password on the command line, you are prompted for it. Best security practice is to provide the password in response to a prompt.

**profile\_mode=OUTBOUND | INBOUND | BOTH**

Optional for the `create` operation only. The direction of the provisioning events. The default is `OUTBOUND` (data is provisioned from Oracle Internet Directory to the application).

**application\_dn=DN**

Required. The distinguished name of the application to which the provisioning subscription belongs. The combination of the application DN and organization DN uniquely identifies a provisioning profile. For example, here is the application DN for Portal:

```
"orclApplicationCommonName=PORTAL,cn=Portal,cn=Products,cn=OracleContext"
```

**application\_type=type**

Required. The type of application being provisioned.

**application\_name=name**

Optional. The name of the application being provisioned. If not provided, defaults to the distinguished name assigned to `application_dn`.

**application\_display\_name=name**

Optional. The display name of the application being provisioned. If not provided, defaults to the value assigned to `application_name`.

**organization\_dn=DN**

Optional. If not provided, defaults to the default identity management realm. The distinguished name of the organization to which the provisioning subscription belongs, for example `"dc=company,dc=com"`. The combination of the application DN and organization DN uniquely identifies a provisioning profile.

**application\_isdasvisible=TRUE | FALSE**

Optional. Determines whether the application is visible as a provisioning-integrated application in the Oracle Internet Directory Provisioning Console. The default value is `TRUE`.

**manage\_application\_default=TRUE | FALSE**

Optional. Determines whether the Oracle Internet Directory Provisioning Console manages the application's default values. The default value is TRUE.

**enable\_bootstrap=TRUE | FALSE**

Optional. Indicates whether the application should receive provisioning events for users that existed in Oracle Internet Directory before creating the application's provisioning integration profile. The default value is FALSE.

**user\_data\_location=DN**

Optional. Identifies the DN of the container in which to store application-specific user information.

**default\_provisioning\_policy=PROVISIONING\_REQUIRED | PROVISIONING\_NOT\_REQUIRED**

Optional. Specifies the application's default provisioning policy. The default value is PROVISIONING\_REQUIRED.

**interface\_name=SCHEMA.PACKAGE**

Required for `create` or `modify` operations. The database schema name for the PLSQL package. The format of the value is `schema.package_name`, for example here is the schema and PLSQL package information for Portal:

```
interface_name=PORTAL.WWSEC_OID_SYNC
```

**interface\_version=1.1 | 2.0 | 3.0**

The version of the interface protocol. Allowed values are 1.1, 2.0, or 3.0. The default value is 2.0.

**interface\_type=PLSQL | JAVA**

Optional. The type of interface to which events will be propagated. The default is PLSQL.

**interface\_connect\_info=connection\_string**

Required for `create` or `modify` operations. To connect to an Oracle database and propagate events, use one of the following formats for the connection string:

- `DBURL=ldap://ldaphost:ldapport/service:username:password` (recommended)
- `host:port:sid:username:password`
- `DBSVC=service:username:password`

**schedule=number\_seconds**

Optional for `create` and `modify` operations only. The number of seconds between executions of this profile. The default is 3600, which means the profile is scheduled to be executed every hour.

**lastchangenumber=number**

Optional for `create` and `modify` operations on `OUTBOUND` events only. The last change number in Oracle Internet Directory after which all qualifying events should be provisioned to the application. Defaults to the latest current change number.

**max\_prov\_failure\_limit=number**

Optional. Determines the number of times the Oracle Provisioning System attempts to provision a user. The default is 1.

**max\_events\_per\_schedule=number**

Optional for `create` and `modify` operations only. The maximum number of events that the Oracle directory integration platform server sends to an application during one execution of a provisioning profile. The default is 100.

**max\_events\_per\_invocation=number**

Optional for `create` and `modify` operations only. The maximum number of events that can be packaged and sent to a target in one invocation of the interface.

**event\_mapping\_rules="OBJECT\_TYPE:FILTER:DOMAIN"**

Required for `create` and `modify` operations on `INBOUND` events only. This rule maps the object type received from the application (using an optional filter condition) to a domain in Oracle Internet Directory A provisioning profile can have multiple mapping rules defined.

The following example shows two mapping rules. The first rule shows that an employee object (`EMP`) whose locality attribute equals America (`l=AMERICA`) should be mapped to the domain `l=AMER, cn=users, dc=company, dc=com`. The second rule shows that an employee object (`EMP`) should be mapped to the domain `cn=users, dc=company, dc=com` (no filter conditions).

```
event_mapping_rules="EMP:l=AMERICA:l=AMER, cn=users, dc=company, dc=com"
event_mapping_rules="EMP::cn=users, dc=company, dc=com"
```

**event\_permitted\_operations="OBJECT:DOMAIN:OPERATION(attributes,...)"**

Required for `create` and `modify` operations on `INBOUND` events only. This property is used to define the types of events that the application is allowed to send to the Oracle Directory Integration Platform service. A provisioning profile can have multiple permitted operations defined.

For example, if you wanted to permit the application to send events whenever a user object was added or deleted, or when certain attributes were modified, you would have three permitted operations such as this:

```
event_permitted_operations="USER:dc=mycompany, dc=com:ADD(*) "
event_permitted_operations="USER:dc=mycompany, dc=com:MODIFY(cn, sn, mail, password) "
event_permitted_operations="USER:dc=mycompany, dc=com:DELETE(*) "
```

**event\_subscription="USER | GROUP:DOMAIN:OPERATION(attributes,...)"**

Required for `create` and `modify` operations on `OUTBOUND` events only. This property is used to define the types of events that the Oracle Directory Integration Platform service should send to the application. A provisioning profile can have multiple event subscriptions defined.

For example, if you wanted the directory integration server to send events to the application whenever a user or group object was added or deleted, you would have four event subscriptions such as this:

```
event_subscription="GROUP:dc=mycompany, dc=com:ADD(*) "
event_subscription="GROUP:dc=mycompany, dc=com:DELETE(*) "
event_subscription="USER:dc=mycompany, dc=com:ADD(*) "
event_subscription="USER:dc=mycompany, dc=com:DELETE(*) "
```

**max\_events\_per\_schedule=number**

Optional for `create` and `modify` operations only. The maximum number of events to be provisioned in one schedule. The default is 100.

**max\_retries=number**

Optional for `create` and `modify` operations only. The number of times a failed event should be retried. The default is 5.

**profile\_group=number**

Required for `create` and `modify` operations only. The group number of the profile. Default is "DEFAULT". This is required to address scalability issues when different Oracle Directory Integration Platform server instances will be used to execute different selected groups.

**profile\_status=ENABLED | DISABLED**

Required for the `create` operation only. Determines whether the profile is enabled or disabled. The default is ENABLED.

**profile\_debug=debug\_level**

Required. The debug level for the profile.

---



---

**Note:** To log all information for a provisioning profile, including entries that are provisioned, set the `profile_debug=debug_level` to a value of 63 for 10g and to a value of 64 for 11g using the `oidprovtool` command.

---



---

## 5.6.3 Tasks and Examples for oidprovtool

Using the Provisioning Registration Tool (`oidprovtool`) you can perform the following tasks:

- [Section 5.6.3.1, "Creating a Provisioning Profile"](#)
- [Section 5.6.3.2, "Modifying a Provisioning Profile"](#)
- [Section 5.6.3.3, "Deleting a Provisioning Profile"](#)
- [Section 5.6.3.4, "Disabling a Provisioning Profile"](#)

### 5.6.3.1 Creating a Provisioning Profile

The following example creates a new provisioning profile that makes Portal aware of updates to the user and group information that is maintained in Oracle Internet Directory.

**Example:**

```
oidprovtool operation=create ldap_host=myhost.mycompany.com ldap_port=3060 \
ldap_user_dn="cn=orcladmin"
application_dn="orclApplicationCommonName=PORTAL,cn=Portal,cn=Products,cn=OracleCo
ntext" \
organization_dn="dc=us,dc=mycompany,dc=com" interface_name=PORTAL.WWSEC_OID_SYNC \
interface_type=PLSQL interface_connect_info=myhost:1521:iasdb:PORTAL:password \
schedule=360 event_subscription="USER:dc=us,dc=mycompany,dc=com:DELETE" \
event_subscription="GROUP:dc=us,dc=mycompany,dc=com:DELETE" \
event_subscription="USER:dc=us,dc=mycompany,dc=com:MODIFY(orclDefaultProfileGroup,
userpassword)" \
```

```
event_subscription="GROUP:dc=us,dc=mycompany,dc=com:MODIFY(uniqueMember)" \
profile_mode=OUTBOUND
```

### 5.6.3.2 Modifying a Provisioning Profile

The following example modifies an existing provisioning profile for the Portal application. It changes the event subscription for the attributes that are provisioned when a user entry is modified.

#### Example:

```
oidprovtool operation=modify ldap_host=myhost.mycompany.com ldap_port=3060 \
ldap_user_dn="cn=orcladmin"
application_dn="orclApplicationCommonName=PORTAL,cn=Portal,cn=Products,cn=OracleCo
ntext" \
organization_dn="dc=us,dc=mycompany,dc=com" \
subscription="USER:dc=us,dc=mycompany,dc=com:MODIFY(orclDefaultProfileGroup,userpa
ssword,mail,cn,sn)"
```

### 5.6.3.3 Deleting a Provisioning Profile

The following example disables a provisioning profile for the Portal application.

#### Example:

```
oidprovtool operation=delete ldap_host=myhost.mycompany.com ldap_port=3060 \
ldap_user_dn="cn=orcladmin"
application_dn="orclApplicationCommonName=PORTAL,cn=Portal,cn=Products,cn=OracleCo
ntext" \
organization_dn="dc=us,dc=mycompany,dc=com"
```

### 5.6.3.4 Disabling a Provisioning Profile

The following example disables a provisioning profile for the Portal application.

#### Example:

```
oidprovtool operation=disable ldap_host=myhost.mycompany.com ldap_port=3060 \
ldap_user_dn="cn=orcladmin"
application_dn="orclApplicationCommonName=PORTAL,cn=Portal,cn=Products,cn=OracleCo
ntext" \
organization_dn="dc=us,dc=mycompany,dc=com"
```

## 5.7 dipStatus

The `dipStatus` utility allows you to check the status of Oracle Directory Integration Platform and whether it is registered.

### 5.7.1 Syntax for dipStatus

#### dipStatus

```
dipStatus -h HOST -p PORT -D wlsuser [-ssl -keystorePath PATH_TO_KEYSTORE
-keystoreType TYPE] [-help]
```

## 5.7.2 Arguments for dipStatus

**-h | -host**

Host name of the WebLogic server running the Managed Server where Oracle Directory Integration Platform is deployed.

**-p | -port**

Listen port of Oracle WebLogic Managed Server where Oracle Directory Integration Platform application is deployed.

**-D | -wlsuser**

WebLogic Server login ID.

---

---

**Note:** You are prompted for the WebLogic server login password. You cannot provide the password as a command-line argument.

Best security practice is to provide a password only in response to a prompt from the command. If you must execute `dipStatus` from a script, you can redirect input from a file containing the WebLogic Server password. Use file permissions to protect the file and delete it when it is no longer necessary.

---

---

**-ssl**

Executes the command in SSL mode.

---

---

**Note:** The Oracle WebLogic Managed Server where Oracle Directory Integration Platform is deployed must be configured for SSL to execute this command in SSL mode. Refer to the *Configuring SSL* chapter in *Oracle Fusion Middleware Securing Oracle WebLogic Server* for more information.

---

---

**-keystorePath**

The full path to the keystore.

**-keystoreType**

The type of the keystore identified by `-keystorePath`. For example: `-keystorePath jks` or `-keystorePath PKCS12`

**-help**

Provides usage help for the command.

## 5.7.3 Examples for dipStatus

```
dipStatus -h myhost.mycompany.com -p 7005 -D weblogic
```

```
dipStatus -help
```



## 5.8 schemasync

The `schemasync` utility enables you to synchronize schema elements—namely attributes and object classes—between an Oracle Internet Directory server and a third-party LDAP directory.

The errors that occur during schema synchronization are logged in the following files:

- `ORACLE_HOME/ldap/odi/log/attributetypes.log`
- `ORACLE_HOME/ldap/odi/log/objectclasses.log`

### 5.8.1 Syntax for schemasync

#### **schemasync**

```
schemasync -srchost hostname -srcport port -srcdn bindDN -srcpwd password
-dsthost hostname -dstport port -dstdn bindDN -dstpwd password [-ldap]
```

### 5.8.2 Arguments for schemasync

#### **-srchost hostname**

Required. The host name of the source directory server.

#### **-srcport port**

Required. The LDAP listening port of the source directory server, for example 3060.

#### **-srcdn bindDN**

Required. The DN of the user used to bind to the source directory. This user must have permissions to modify the directory schema, for example the superuser (cn=orcladmin).

#### **-srcpwd password**

Optional. The user password used to bind to the source directory. If you do not specify the password on the command line, you are prompted for it. Best security practice is to provide the password in response to a prompt.

#### **-dsthost hostname**

Required. The host name of the destination directory server.

#### **-dstport port**

Required. The LDAP listening port of the destination directory server, for example 3060.

#### **-dstdn bindDN**

Optional. The DN of the user used to bind to the destination directory. This user must have permissions to modify the directory schema, for example the superuser.

#### **-dstpwd password**

Required. The user password used to bind to the destination directory. If you do not specify the password on the command line, you are prompted for it. Best security practice is to provide the password in response to a prompt.

**-ldap**

Optional. If specified, then the schema changes are applied directly from the source LDAP directory to the destination LDAP directory. If it is not specified, then the schema changes are placed in the following LDIF files:

- `ORACLE_HOME/ldap/odi/data/attributetypes.ldif`: This file has the new attribute definitions.
- `ORACLE_HOME/ldap/odi/data/objectclasses.ldif`: This file has the new object class definitions.

If you do not specify `-ldap`, then you must use [Section 3.11, "ldapmodify"](#) to upload the definitions from these two files, first attribute types and then object classes.

### 5.8.3 Tasks and Examples for schemasync

Using the `schemasync` command-line tool, you can perform the following tasks:

- [Section 5.8.3.1, "Synchronizing the Schema between Oracle Internet Directory and a Third-Party Directory"](#)
- [Section 5.8.3.2, "Comparing the Schema between two Oracle Internet Directory Servers"](#)
- [Section 5.8.3.3, "Synchronizing the Schema between two Oracle Internet Directory Servers"](#)

#### 5.8.3.1 Synchronizing the Schema between Oracle Internet Directory and a Third-Party Directory

The following example shows how to synchronize the schema between Oracle Internet Directory and a third-party directory server.

**Example:**

```
schemasync -srchost myhost1.mycompany.com -srcport 3060 -srcdn "cn=orcladmin" \  
-dsthost myhost2.mycompany.com -dstport 3060 \  
-dstdn "uid=superuser,ou=people,dc=mycompany,dc=com" -ldap
```

#### 5.8.3.2 Comparing the Schema between two Oracle Internet Directory Servers

Use the `schemasync` command-line tool to compare two OID's schemas:

**Example:**

```
schemasync -srchost myhost1.mycompany.com -srcport 3060 -srcdn "cn=orcladmin" \  
-dsthost myhost2.mycompany.com -dstport 3060 "cn=orcladmin"
```

#### 5.8.3.3 Synchronizing the Schema between two Oracle Internet Directory Servers

Use the `schemasync` command-line tool to synchronize an OID server schema to another OID server:

**Example:**

```
schemasync -srchost myhost1.mycompany.com -srcport 3060 -srcdn "cn=orcladmin" \  
-dsthost myhost2.mycompany.com -dstport 3060 "cn=orcladmin" -ldap
```

### 5.8.4 Related Command-Line Tools for schemasync

- See [Section 3.11, "ldapmodify"](#)

# Part II

---

## Schema Reference

Part II of the *Oracle Fusion Middleware Reference for Oracle Identity Management* contains information about the LDAP schema elements for Oracle Identity Management.

Part II contains the following chapters:

- [Chapter 6, "LDAP Schema Overview"](#)
- [Chapter 7, "LDAP Object Class Reference"](#)
- [Chapter 8, "LDAP Attribute Reference"](#)



---

---

## LDAP Schema Overview

This chapter describes the basic concepts of the LDAP directory schema and provides detailed lists of the schema elements for Oracle Identity Management.

This chapter includes the following sections:

- Section 6.1, "Overview of Directory Schema"
- Section 6.2, "Overview of Oracle Identity Management Schema Elements"

### 6.1 Overview of Directory Schema

A directory schema specifies, among other rules, the types of objects that a directory may have and the mandatory and optional attributes of each object type. The Lightweight Directory Access Protocol (LDAP) version 3 defines a schema based on the X.500 standard for common objects found in a network, such as countries, localities, organizations, people, groups, and devices. In the LDAP v3, the schema is available from the directory. That is, it is represented as entries in the directory and its information as attributes of those entries.

This section contains the following topics:

- Section 6.1.1, "Object Classes"
- Section 6.1.2, "Attributes"
- Section 6.1.3, "LDAP Controls"

#### 6.1.1 Object Classes

An object class is an LDAP directory term that denotes the type of object being represented by a directory entry or record. There are also object classes that define an object's relationship to other objects, such as object class `top` denotes that the object may have subordinate objects under it in a hierarchical tree structure. Some LDAP object classes may be combined to create an entry in the directory. For example, an entry for a user uses the `top`, `person`, `organizationalPerson`, `inetOrgPerson`, and `orclUserV2` object classes.

##### Required and Allowed Attributes

The definition of an object class includes a list of required attributes (MUST) and allowed attributes (MAY). Required attributes include the attributes that must be present in entries using the object class. Allowed attributes include the attributes that may be present in entries using the object class.

### Object Class Types

The X.500 1993 specification requires that object classes be assigned to one of four categories:

- **Structural:** Object classes that can have instances in the directory. Structural classes are used to create directory objects or entries.
- **Abstract:** Template object classes that are used only to derive new structural classes. Abstract classes cannot be instantiated in the directory.
- **Auxiliary:** A list of attributes that can be appended to the definition of a Structural or Abstract class. An Auxiliary class cannot be instantiated in the directory.
- **88 Classes:** Assigning object classes to categories was not required in the X.500 1988 specification. Classes that were defined prior to the X.500 1993 standards, default to the 88 class. Do not define new 88 classes.

### Object Class Inheritance

Inheritance, which is also referred to as derivation, is the ability to build new object classes from existing object classes. The new object is defined as a subclass of the parent object. A subclass is a class that inherits from some other class; for example, a subclass inherits structure and content rules from the parent. The parent object becomes a superclass of the new object. A superclass is a class from which one or more other classes inherit information.

## 6.1.2 Attributes

Directory data is represented as attribute-value pairs. Any piece of information in the directory is associated with a descriptive attribute. For example, the `cn` (`commonName`) attribute is used to store a nickname. A person named William (Bill) Smith can be represented in the directory as:

```
cn: Bill Smith
```

### Attribute Name Limitations

The length of an attribute name must not exceed 127 characters. For more information about attribute management, refer to the *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*.

Oracle Internet Directory imposes no limitations on the characters that can be used in attribute names. Other components of Oracle Identity Management, however, do limit the characters that can be used for certain attributes.

Oracle Delegated Administration Services and Oracle Directory Integration Platform prohibit the use of spaces and of any of the following characters in `UserID`: `& ' % ? \ / + = ( ) * ^ , ; | ' ~`

Oracle Application Server Single Sign-On requires that a password should not contain the following characters: `& { } < > " ' ( )`

### Attribute Syntax

An attribute syntax is the basic building block of an attribute. Every attribute is assigned a syntax that defines the attribute value's data format. For example, attribute syntaxes determine whether an attribute stores an integer, string, or binary data. The syntax also defines the matching rules that control the type of comparison operations you can perform on the attribute value.

Oracle Internet Directory recognizes attribute syntax as specified in RFC 2252, that is, it enables you to associate the attribute syntax described in that document with an attribute. Oracle Internet Directory enforces attribute syntax for the following types:

- DN
- OID (object identifier)
- Telephone Number

The following table describes the attribute syntax most commonly used in Oracle Internet Directory:

**Table 6–1 Attribute Syntax Commonly Used in Oracle Internet Directory**

Syntax and Object ID	Description
ACI Item 1.3.6.1.4.1.1466.115.121.1.1	Values for this attribute are access control identifier items.
Binary 1.3.6.1.4.1.1466.115.121.1.5	Values for this attribute are binary.
Boolean 1.3.6.1.4.1.1466.115.121.1.7	The attribute can contain only one of two values: true (1) or false (0).
Directory String 1.3.6.1.4.1.1466.115.121.1.15	Values for this attribute are strings which are not case-sensitive.
DN 1.3.6.1.4.1.1466.115.121.1.12	Values for this attribute are DNs (distinguished names).
Generalized Time 1.3.6.1.4.1.1466.115.121.1.24	Values for this attribute are encoded as printable strings. A time zone must be specified (such as GMT).
IA5String 1.3.6.1.4.1.1466.115.121.1.26	International Reference Alphabet Reference Alphabet No. 5 string. Values for this attribute are case-sensitive.
Integer 1.3.6.1.4.1.1466.115.121.1.27	Valid values for this attribute are numbers.
JPEG 1.3.6.1.4.1.1466.115.121.1.28	Valid values for this attribute are JPEG files.
Name 1.3.6.1.4.1.1466.115.121.1.34	Valid values for this attribute are names or optional UIDs.
OID 1.3.6.1.4.1.1466.115.121.1.38	A unique object identifier.
Printable String 1.3.6.1.4.1.1466.115.121.1.44	A string that does NOT allow extended characters. Values for this attribute are not case-sensitive.
Telephone Number 1.3.6.1.4.1.1466.115.121.1.50	Values for this attribute are in the form of telephone numbers.

### Attribute Aliases

As of 11g Release 1 (11.1.1), you can create aliases for attribute names. For example, you could create the user-friendly alias `surname` for the attribute `sn`. Once you create an alias for an attribute name, a user can specify the alias instead of the attribute name in an LDAP operation.

You define an alias for an attribute in the LDAP schema definition of the attribute. The directory schema operational attribute `attributeTypes` has been enhanced to allow you to include aliases in the attribute name list. In previous releases, the format for an attribute name list was:

```
attributeTypes=( ObjectIdentifier NAME 'AttributeName' ... )
```

As of 11g Release 1 (11.1.1), you may optionally specify:

```
attributeTypes=( ObjectIdentifier NAME ( 'AttributeName' 'Alias1' 'Alias2' ...) ... )
```

This is consistent with the LDAP protocol as specified by RFC 2251 and RFC 2252. In the attribute name list, the first item is recognized as the name of the attribute and rest of the items in the list are recognized as attribute aliases. For example, to specify the alias `surname` for the attribute `sn`, you would change the schema definition for `sn` from:

```
attributeTypes=( 2.5.4.4 NAME 'sn' SUP name )
```

to:

```
attributeTypes=( 2.5.4.4 NAME ( 'sn' 'surname' ) SUP name )
```

**See Also:** For more information regarding attribute alias rules, managing attribute aliases using command-line tools, and using attribute aliases refer to the "Attribute Aliases In the Directory" section in *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*

### Matching Rules

Matching rules are the rules for matching two attribute values that comply with the same attribute syntax. Oracle Internet Directory recognizes the following matching rule definitions in the schema.

- `accessDirectiveMatch`
- `IntegerMatch`
- `bitStringMatch`
- `numericStringMatch`
- `caseExactMatch`
- `objectIdentifierFirstComponentMatch`
- `caseExactIA5Match`
- `ObjectIdentifierMatch`
- `caseIgnoreIA5Match`
- `OctetStringMatch`
- `caseIgnoreListMatch`
- `presentationAddressMatch`
- `caseIgnoreMatch`
- `protocolInformationMatch`
- `caseIgnoreOrderingMatch`
- `telephoneNumberMatch`



- distinguishedNameMatch
- uniqueMemberMatch
- generalizedTimeMatch
- generalizedTimeOrderingMatch
- orclpkimatchingrule

Of the matching rules in the previous list, Oracle Internet Directory actually enforces the following when it compares attribute values:

- distinguishedNameMatch
- caseExactMatch
- caseIgnoreMatch
- numericStringMatch
- IntegerMatch
- telephoneNumberMatch
- orclpkimatchingrule

### Sizing of Attribute Values

Attribute syntax does not put any specific size constraint on attribute values. You can, however, specify the size of the attribute value when defining the attribute. Some attributes in Oracle Internet Directory may have size constraints defined, however length characteristics of an attribute are not enforced.

For example, this syntax limits the attribute `foo` size to 64, but this size limit is not enforced in Oracle Internet Directory:

```
(object_identifier_of_attribute NAME 'foo' EQUALITY caseIgnoreMatch SYNTAX
'object_identifier_of_syntax{64}' )
```

### Single-Valued and Multi-Valued Attributes

By default, most attributes are multi-valued. This means that an entry can contain the same attribute with multiple values. For single-valued attributes, only one instance of the attribute can be specified in an entry. For example, the attribute `orclObjectGUID` attribute can only have one possible value.

### Attribute Usage

Attribute Usage defines how the attribute is used in the directory. The attribute usage types are:

- **User applications attribute**—Default attribute usage if not explicitly defined for the attribute.
- **System Operational attribute**—Attributes that control operation of the directory itself.

**See Also:** "Managing System Operational Attributes" in *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*

### Not User Modifiable

Attributes that are designated as "not user modifiable" can only be modified by the directory server. They cannot be modified by any other user or process.

### 6.1.3 LDAP Controls

As an LDAP Version 3 directory, Oracle Internet Directory extends the standard LDAP operations by using controls. These are extra pieces of information carried along with existing operations, altering the behavior of the operation. When a client application passes a control along with the standard LDAP command, the behavior of the commanded operation is altered accordingly.

The controls supported by Oracle Internet Directory 11g Release 1 (11.1.1) are listed in [Table 6–2, "Request Controls Supported by Oracle Internet Directory"](#) and [Table 6–3, "Response Controls Supported by Oracle Internet Directory"](#).



**Table 6–2 Request Controls Supported by Oracle Internet Directory**

Object Identifier	Name	Description
2.16.840.1.113730.3.4.18	Proxy Authorization	<p>Allows an LDAP client application to bind to Oracle Internet Directory server with its own identity and then to perform operations on behalf of another user or on behalf of multiple users.</p> <p>This control can improve performance especially for proxy operations performed on behalf of multiple users. The LDAP operation does not require a rebind for each user.</p> <p>For example, consider this scenario:</p> <ol style="list-style-type: none"> <li>1. A client application named <code>proxy-app</code> binds to Oracle Internet Directory server.</li> <li>2. A user named John Doe sends a request to the <code>proxy-app</code> client application. The client must be a member of the proxy authorization group.</li> <li>3. Instead of passing the request to the Oracle Internet Directory server as <code>proxy-app</code>, the client passes the Proxy Authorization control along with the proxy dn (John Doe) to the server.</li> <li>4. The server performs the LDAP request for John Doe using John Doe's privileges (ACLs). The server can access only the information or perform only the operations that John Doe has privileges to access or perform.</li> </ol> <p>Considerations for the Proxy Authorization control are:</p> <ul style="list-style-type: none"> <li>■ If the control is not accompanied by a proxy dn, the server throws an exception and returns an error to the client. If the criticality flag is not set to TRUE, the request is rejected with a protocol error.</li> <li>■ If the proxy user has the privileges to perform the operation as per the ACLs, the server executes the request; otherwise, the server returns the result code "123".</li> <li>■ Oracle Internet Directory server determines if a Proxy Authorization request is to be honored. Anonymous users are not allowed to assume the identity of others.</li> <li>■ If the server receives more than one Proxy Authorization control in the same operation, an error is returned to the client application and the operation attempt is unsuccessful.</li> </ul>

**Table 6–2 (Cont.) Request Controls Supported by Oracle Internet Directory**

Object Identifier	Name	Description
1.3.6.1.4.1.42.2.27.8.5.1	Password Policy	<p>Allows an LDAP client to request information from Oracle Internet Directory server about the current password policy state for a user. If a password policy is applicable, a client can send this control with these operations:</p> <ul style="list-style-type: none"> <li>■ ldapbind, ldapmodify, ldapadd, or ldapcompare</li> <li>■ ldapsearch</li> </ul> <p>Other operations such as ldapunbind and ldapabandon are not supported. Also, this control does not apply to a replication bind.</p> <p>The password policy request control does not have a <code>controlValue</code>, but the response control has return values, which are described in Table 6–3.</p> <p>The password policy is typically applied to the single-valued attribute <code>userPassword</code> for the LDAP simple authentication method or password-based Simple Authentication and Security Layer (SASL) authentication.</p> <p>For more information, see "Password Policy for LDAP Directories" at this location:</p> <p><a href="http://tools.ietf.org/html/draft-behera-ldap-password-policy-09">http://tools.ietf.org/html/draft-behera-ldap-password-policy-09</a></p>
2.16.840.1.113730.3.4.3	Persistent Search	<p>Allows an LDAP client to send a persistent search request to Oracle Internet Directory server.</p> <p>A persistent search operation is an enhanced search that continues after the initial search results are returned by the server to the client. After the initial search is finished, the connection to the server is kept alive until the client unbinds or abandons the operation. The client can track changes for entries in the search scope and receive an Entry Change Notification response control if an entry is modified.</p> <p>The definition for this control is:</p> <pre>PersistentSearch ::= SEQUENCE {     controlType 2.16.840.1.113730.3.4.3     changeTypes INTEGER,     changesOnly BOOLEAN,     returnECs BOOLEAN }</pre> <p>For a description of these fields, see:</p> <p><a href="http://tools.ietf.org/id/draft-ietf-ldapext-psearch-03.txt">http://tools.ietf.org/id/draft-ietf-ldapext-psearch-03.txt</a></p>

**Table 6–2 (Cont.) Request Controls Supported by Oracle Internet Directory**

Object Identifier	Name	Description
2.16.840.1.113894.1.8.39	Computed Attribute Value Uniqueness	<p>Allows computed attribute value uniqueness for an entry-based combination of multiple attribute values. Usually, attribute uniqueness is configured only for a single attribute. An application that requires uniqueness for a combination of attribute values can send this control, and Oracle Internet Directory server ensures that the computed attribute value is unique across the directory during an operation such as <code>ldapadd</code>, <code>ldapmodify -add</code>, or <code>ldapmodify -replace</code>.</p> <p>If an entry with the computed value already exists, Oracle Internet Directory server returns the LDAP error code: <code>LDAP_ALREADY_EXISTS = 0x44</code>.</p> <p>For example, in a multi-tenant environment, the UID attribute of a user must be unique for a specific tenant but not necessarily unique across the directory. An application creates an LDAP entry with a computed attribute named <code>TenantID_UID</code>, where <code>TenantID</code> is the identifier of the tenant and <code>UID</code> is the attribute. The application that creates the LDAP entry sends this control, and if an entry with the computed attribute already value already exists, Oracle Internet Directory server returns the <code>LDAP_ALREADY_EXISTS</code> error code.</p>
2.16.840.1.113730.3.4.9	OID_SEARCH_VLV_REQ_CONTROL	<p>Allows a client to specify that the server return, for a given LDAP search, a contiguous subset of a large search result set. It can be used to go through the search results one page at a time, which allows a client to retrieve results more quickly and prevents the client from needing to store too many search results at a time.</p> <p>The server returns the <code>OID_SEARCH_VLV_RES_CONTROL 2.16.840.1.113730.3.4.10</code>.</p> <p>The <code>OID_SEARCH_VLV_REQ_CONTROL</code> works only in conjunction with the <code>SORT</code> control (<code>ldapsearch -T</code> argument). If you do not include a <code>SORT</code> control, the request returns LDAP error code 53 - Search operation with VLV request control is missing <code>SORT</code> request control.</p> <p>The <code>SORT</code> control can contain any sort specification valid for the server. When the <code>SORT</code> control is used with the <code>OID_SEARCH_VLV_REQ_CONTROL</code>, the server does not return the complete set of sorted search results, but instead returns a contiguous subset of those entries specified in the control using a target entry as a reference point for results.</p> <p>For more information, see "LDAP Extensions for Scrolling View Browsing of Search Results" at <a href="http://tools.ietf.org/html/draft-ietf-ldapext-ldapv3-vlv-09">http://tools.ietf.org/html/draft-ietf-ldapext-ldapv3-vlv-09</a>.</p>
1.2.840.113556.1.4.319	OID_SEARCH_PAGING_CONTROL	See the "Extensions to the LDAP Protocol" chapter in Oracle Fusion Middleware Application Developer's Guide for Oracle Identity Management
1.2.840.113556.1.4.473	OID_SEARCH_SORTING_REQUEST_CONTROL	See the "Extensions to the LDAP Protocol" chapter in Oracle Fusion Middleware Application Developer's Guide for Oracle Identity Management
2.16.840.1.113730.3.4.2	GSL_MANAGE_DSA_CONTROL	Used to manage referrals, dynamic groups, and alias objects in Oracle Internet Directory. For more information, please see RFC 3296, "Named Subordinate References in Lightweight Directory Access Protocol (LDAP) Directories," at <a href="http://www.ietf.org">http://www.ietf.org</a> .

**Table 6–2 (Cont.) Request Controls Supported by Oracle Internet Directory**

Object Identifier	Name	Description
2.16.840.1.113894.1.8.1	OID_RESET_PROXYCONTROL_IDENTITY	Used to perform a proxy switch of an identity on an established LDAP connection. For example, suppose that Application A connects to the directory server and then wishes to switch to Application B. It can simply do a rebind by supplying the credentials of Application B. However, there are times when the proxy mechanism for the application to switch identities could be used even when the credentials are not available. With this control, Application A can switch to Application B provided Application A has the privilege in Oracle Internet Directory to proxy as Application B.
2.16.840.1.113894.1.8.2	OID_APPLYUSEPASSWORD_POLICY	Sent by applications that require Oracle Internet Directory to check for account lockout before sending the verifiers of the user to the application. If Oracle Internet Directory detects this control in the verifier search request and the user account is locked, then Oracle Internet Directory does not send the verifiers to the application. It sends an appropriate password policy error.
2.16.840.1.113894.1.8.3	CONNECT_BY	See the "Extensions to the LDAP Protocol" chapter in Oracle Fusion Middleware Application Developer's Guide for Oracle Identity Management
2.16.840.1.113894.1.8.4	OID_CLIENT_IP_ADDRESS	Intended for a client to send the end user IP address if IP lockout is to be enforced by Oracle Internet Directory.
2.16.840.1.113894.1.8.5	GSL_REQDATTR_CONTROL	Used with dynamic groups. Directs the directory server to read the specific attributes of the members rather than the membership lists.
2.16.840.1.113894.1.8.6	PasswordStatusRequestControl	When packaged as part of the LDAP Bind/Compare operation request, this control causes the server to generate a password policy response control. The actual response control depends on the situation. Cases include imminent password expiration, number of grace logins remaining, password expired, and account locked.
2.16.840.1.113894.1.8.14	OID_DYNAMIC_VERIFIER_REQUEST_CONTROL	The request control that the client sends when it wants the server to create a dynamic password verifier. The server uses the parameters in the request control to construct the verifier.
2.16.840.1.113894.1.8.16	AccountStatusRequestControl	When packaged with the LDAP search operation associated with the authentication process, the Oracle Internet Directory returns a password policy response control to inform the client application of account state related information like account lockout, password expiration etc. The application can then parse and enforce the results.
2.16.840.1.113894.1.8.23	GSL_CERTIFICATE_CONTROL"	Certificate search control. The request control that the client sends to specify how to search for a user certificate. See the appendix "Searching the Directory for User Certificates" in <i>Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory</i> .
2.16.840.1.113894.1.8.29	EffectivePolicyControl	This control is packaged as part of an LDAP base search, where the base DN is that of the user entry being tested. The entry need not exist in the directory at the time. Passing this control results in the return of the LDAP entry describing the applicable password policy, assuming the entity performing the search has the access rights to view the password policy entry. If the desired password is provided as the optional testPassword parameter, the directory server returns the response control 2.16.840.1.113894.1.8.32.

**Table 6–2 (Cont.) Request Controls Supported by Oracle Internet Directory**

<b>Object Identifier</b>	<b>Name</b>	<b>Description</b>
2.16.840.1.113894.1.8.36	DelSubtreeControl	When this control is sent with a delete operation, it causes the deletion of the entire subtree below the DN provided. Any user having necessary privileges can perform this operation.
1.2.840.113556.1.4.805	DelSubtreeControl	When this control is sent with a delete operation, it causes the deletion of the entire subtree below the DN provided. Any user having necessary privileges can perform this operation.
1.3.6.1.1.21.2	TransactionSpecificationControl	This is an LDAPControl indicating association of an operation to a transaction by means of the transaction identifier, which is the value of this control. Its criticality is TRUE.

---



**Table 6–3 Response Controls Supported by Oracle Internet Directory**

Object Identifier	Name	Description
1.3.6.1.4.1.42.2.27.8.5.1	Password Policy	<p>Response control that the Oracle Internet Directory server returns to an LDAP client in response to the Password Policy request control. The response control value is encoded as follows:</p> <pre> PasswordPolicyResponseValue ::= SEQUENCE {   warning [0] CHOICE {     timeBeforeExpiration [0] INTEGER (0 .. maxInt),     graceAuthNsRemaining [1] INTEGER (0 .. maxInt)   } OPTIONAL,   error [1] ENUMERATED {     passwordExpired (0),     accountLocked (1),     changeAfterReset (2),     passwordModNotAllowed (3),     mustSupplyOldPassword (4),     insufficientPasswordQuality (5),     passwordTooShort (6),     passwordTooYoung (7),     passwordInHistory (8) } OPTIONAL } </pre> <p>The server sends either an error or warning in the password policy response control (but not both). Error codes are described in:</p> <p><a href="http://tools.ietf.org/html/draft-behera-ldap-password-policy-09">http://tools.ietf.org/html/draft-behera-ldap-password-policy-09</a></p> <p>Control criticality is not returned in the response. For a non violation of the password policy, the server does not send a response.</p>
2.16.840.1.113730.3.4.7	Entry Change Notification	<p>Returned by the Oracle Internet Directory server to an LDAP client in response to a Persistent Search control that has the returnECs field set to TRUE. This control is returned for each changed entry that matches the persistent search criteria and describes the change made to the specific search entry.</p> <p>The definition for this control is:</p> <pre> EntryChangeNotification ::= SEQUENCE {   controlType 2.16.840.1.113730.3.4.7   changeType ENUMERATED {     add (1),     delete (2),     modify (4),     modDN (8)   },   previousDN LDAPDN OPTIONAL, --   modifyDN ops. only   changeNumber INTEGER OPTIONAL -- if   supported } </pre> <p>For a description of these fields, see:</p> <p><a href="http://tools.ietf.org/id/draft-ietf-ldapext-psearch-03.txt">http://tools.ietf.org/id/draft-ietf-ldapext-psearch-03.txt</a></p>
2.16.840.1.113730.3.4.10	OID_SEARCH_VLV_RES_C ONTROL	<p>The server sends this control in response to an OID_SEARCH_VLV_REQ_CONTROL 2.16.840.1.113730.3.4.9.</p>

**Table 6–3 (Cont.) Response Controls Supported by Oracle Internet Directory**

Object Identifier	Name	Description
2.16.840.1.113894.1.8.7	OID_PASSWORD_EXPWARNING_CONTROL	Password policy control. Response control that the server sends when the pwdExpireWarning attribute is enabled and the client sends the request control. The response control value contains the time in seconds to password expiration.
2.16.840.1.113894.1.8.8	OID_PASSWORD_GRACE_LOGIN_CONTROL	Password policy control. The response control that the server sends when grace logins are configured and the client sends a request control. The response control value contains the remaining number of grace logins.
2.16.840.1.113894.1.8.20	OID_PWDEXPIRED_CONTROL	Password policy control. The response control that the server sends when the password has expired, there are no grace logins remaining, and the client sends a request control.
2.16.840.1.113894.1.8.9	OID_PASSWORD_MUST_CHANGE_CONTROL	Password policy control. The response control that the server sends when forced password reset is enabled and the client sends the request control. The client must force the user to change the password upon receipt of this control.
2.16.840.1.113894.1.8.15	OID_DYNAMIC_VERIFIER_RESPONSE_CONTROL	The response control that the server sends to the client when an error occurs. The response control contains the error code.
2.16.840.1.113894.1.8.32	PasswordValidationControl	The server sends this in response to control 2.16.840.1.113894.1.8.29 when the desired password is provided as the optional testPassword parameter. A client application can parse the validationResult to determine whether the password can be accepted by the server ("Success") or the reason it has been rejected. The same type of error message generated during a failed LDAP modify operation on userpassword is returned as the value.
2.16.840.1.113894.1.8.37	OID_SEARCH_DYNGRP_STATIC_UMEM	When you send a query with filter (unique)member=value along with this control, then the server provides search results with entries that includes only the static (unique)members.

## 6.2 Overview of Oracle Identity Management Schema Elements

This section lists the Oracle Identity Management schema elements by category. Each category contains a list of applicable LDAP object classes and attributes that link to the detailed information for the specified attribute or object class. The schema elements are grouped into the following categories:

- [Section 6.2.1, "System Operational Schema Elements"](#)
- [Section 6.2.2, "Oracle Internet Directory Configuration Schema Elements"](#)
- [Section 6.2.3, "Audit and Error Logging Schema Elements"](#)
- [Section 6.2.4, "Server Manageability Schema Elements"](#)
- [Section 6.2.5, "Oracle Directory Replication Schema Elements"](#)
- [Section 6.2.6, "Oracle Directory Integration and Provisioning Schema Elements"](#)
- [Section 6.2.7, "Oracle Delegated Administration Services Schema Elements"](#)
- [Section 6.2.8, "Oracle Application Server Certificate Authority and PKI Schema Elements"](#)

- [Section 6.2.9, "Application Schema Elements"](#)
- [Section 6.2.10, "Resource Schema Elements"](#)
- [Section 6.2.11, "Plug-in Schema Elements"](#)
- [Section 6.2.12, "Directory User Agents Schema Elements"](#)
- [Section 6.2.13, "User, Group, and Subscriber Schema Elements"](#)
- [Section 6.2.14, "Password Policy Schema Elements"](#)
- [Section 6.2.15, "Password Verifier Schema Elements"](#)

## 6.2.1 System Operational Schema Elements

System operational schema elements are those used by the directory server. System operational object classes are used by the directory server to create entries that pertain to directory server operations. Certain system operational attributes may be available for use on every entry in the directory, regardless of whether they are defined for the object class of the entry. This section contains the following topics:

- [Section 6.2.1.1, "Directory Schema"](#)
- [Section 6.2.1.2, "Access Control"](#)
- [Section 6.2.1.3, "Change Logs"](#)
- [Section 6.2.1.4, "Password Policy"](#)

### 6.2.1.1 Directory Schema

This section lists the operational attributes and object classes for the directory schema.

#### Attributes

[attributeTypes](#), [contentRules](#), [ldapSyntaxes](#), [matchingRules](#), [objectClasses](#)

#### Object Classes

[subschema](#)

### 6.2.1.2 Access Control

This section lists the operational attributes for access control.

#### Attributes

[orclACI](#), [orclEntryLevelACI](#)

### 6.2.1.3 Change Logs

This section lists the operational attributes for change logs.

#### Attributes

[createTimestamp](#), [creatorsName](#), [modifiersName](#), [modifyTimestamp](#)

### 6.2.1.4 Password Policy

This section lists the operational attributes for password policy.

**Attributes**

orclPwdAccountUnlock, orclPwdIPAccountLockedTime, orclPwdIPFailureTime, orclRevPwd, orclUnsyncRevPwd, pwdAccountLockedTime, pwdChangedTime, pwdExpirationWarned, pwdFailureTime, pwdGraceUseTime, pwdHistory, pwdReset

## 6.2.2 Oracle Internet Directory Configuration Schema Elements

This section lists the schema elements that pertain to the configuration of Oracle Internet Directory. It contains the following topics:

- Section 6.2.2.1, "Oracle Internet Directory Server"
- Section 6.2.2.2, "Oracle Context"
- Section 6.2.2.3, "Oracle Network Services"
- Section 6.2.2.4, "Garbage Collection"
- Section 6.2.2.5, "Attribute Uniqueness"

### 6.2.2.1 Oracle Internet Directory Server

This section lists the attributes and object classes that pertain to the configuration of Oracle Internet Directory server.

**Attributes**

namingContexts, orclAnonymousBindsFlag, orclCatalogEntryDN, orclCompatibleVersion, orclCryptoScheme, orclDBType, orclDebugFlag, orclDebugForceFlush, orclDebugOp, orclDIPRepository, orclDirectoryVersion, orclDITRoot, orclEcacheEnabled, orclEcacheMaxEntries, orclEcacheMaxSize, orclEnableGroupCache, orclEventLevel, orclGUPassword, orclHostname, orclIndexedAttribute, orclIpAddress, orclLDAPConnTimeout, orclMatchDnEnabled, orclMaxCC, orclNonSSLPort, orclNormDN, orclNwrvTimeout, orclPKIMatchingRule, orclPrName, orclPrPassword, orclReplAgreements, orclReplicaID, orclSASLAuthenticationMode, orclSASLCipherChoice, orclSASLMechanism, orclsDumpFlag, orclServerMode, orclServerProcs, orclSizeLimit, orclSkewedAttribute, orclSkipRefInSQL, orclSSLAuthentication, orclSSLCipherSuite, orclSSLEnable, orclSSLPort, orclSSLVersion, orclSSLWalletURL, orclStatsDN, orclStatsFlag, orclStatsLevel, orclStatsOp, orclStatsPeriodicity, orclSUAccountLocked, orclSuffix, orclSULoginFailureCount, orclSUName, orclSUPassword, orclTimeLimit, orclTLimitMode, orclUpgradeInProgress

**Object Classes**

orclDSAConfig, orclIndexOC, orclLDAPInstance, orclLDAPSubConfig, subentry, subregistry

### 6.2.2.2 Oracle Context

This section lists the attributes and object classes that pertain to the configuration of the Oracle Context.

**Attributes**

orclCommonAutoRegEnabled, orclCommonContextMap, orclCommonDefaultUserCreateBase, orclCommonGroupCreateBase, orclCommonNamingAttribute, orclCommonNicknameAttribute, orclCommonSASLRealm, orclCommonUserSearchBase, orclDefaultSubscriber,

orclProductVersion, orclSubscriberNickNameAttribute, orclSubscriberSearchBase, orclUserObjectClasses, orclVersion

### Object Classes

orclCommonAttributes, orclCommonAttributesV2, orclRootContext, orclSchemaVersion

### 6.2.2.3 Oracle Network Services

This section lists the attributes and object classes that pertain to the configuration of Oracle Network Services.

#### Attributes

labeledURI, orclActiveEndDate, orclActiveStartdate, orclAssocDB, orclAssocIasInstance, orclEnabled, orclFlexAttribute1, orclIsEnabled, orclMasterNode, orclNetDescName, orclNetDescString, orclOracleHome, orclServiceInstanceLocation, orclServiceMember, orclServiceSubscriptionLocation, orclServiceSubType, orclServiceType, orclSID, orclSuiteType, orclSystemName, orclVersion

#### Object Classes

orclService, orclServiceInstance, orclServiceInstanceReference, orclServiceRecipient, orclServiceSuite, orclServiceSubscriptionDetail

### 6.2.2.4 Garbage Collection

This section lists the attributes and object classes that pertain to the configuration of garbage collection.

#### Attributes

orclPurgeBase, orclPurgeDebug, orclPurgeEnable, orclPurgeFileLoc, orclPurgeFileName, orclPurgeFilter, orclPurgeInterval, orclPurgeNow, orclPurgePackage, orclPurgeStart, orclPurgeTargetAge, orclPurgeTranSize

#### Object Classes

orclPurgeConfig, tombstone

### 6.2.2.5 Attribute Uniqueness

This section lists the attributes and object classes that pertain to the configuration of attribute uniqueness.

#### Attributes

orclUniqueAttrName, orclUniqueEnable, orclUniqueObjectClass, orclUniqueScope, orclUniqueSubtree

#### Object Classes

orclUniqueConfig

## 6.2.3 Audit and Error Logging Schema Elements

This section lists the attributes and object classes that pertain to audit logs and error logs.

**Attributes**

orclAuditAttribute, orclAuditMessage, orclDBConnCreationFailed, orclDNSUnavailable, orclEventTime, orclEventType, orclFDIncreaseError, orclMaxFDLimitReached, orclMaxProcessLimitReached, orclMemAllocError, orclNWCongested, orclNwUnavailable, orclOpResult, orclORA28error, orclORA3113error, orclORA3114error, orclSequence, orclThreadSpawnFailed, orclUserDN

**Object Classes**

orclAuditOC, orclEventLog, orclEvents, orclSysResourceEvents

## 6.2.4 Server Manageability Schema Elements

This section lists the schema elements for Oracle Internet Directory server manageability statistics.

**Attributes**

orclACLResultsLatency, orclActiveConn, orclActiveThreads, orclAttrACLEvalLatency, orclAuditMessage, orclBERgenLatency, orclDBLatency, orclDIMEonlyLatency, orclEcacheHitRatio, orclEcacheNumEntries, orclEcacheSize, orclEntryACLEvalLatency, orclEventTime, orclEventType, orclFilterACLEvalLatency, orclFrontLatency, orclGenObjLatency, orclGetNearACLLatency, orclHostname, orclIdleConn, orclIdleThreads, orclInitialServerMemSize, orclIpAddress, orclLDAPInstanceID, orclLDAPPProcessID, orclOpAbandoned, orclOpCompleted, orclOpenConn, orclOpFailed, orclOpInitiated, orclOpLatency, orclOpPending, orclOpResult, orclOpSucceeded, orclOpTimedOut, orclQueueDepth, orclQueueLatency, orclReadWaitThreads, orclSequence, orclServerAvgMemGrowth, orclSMSpec, orclSQLexeFetchLatency, orclSQLGenReusedParsed, orclTcpConnToClose, orclTcpConnToShutDown, orclTotFreePhyMem, orclTraceDimensionLevel, orclTraceFileLocation, orclTraceFileSize, orclTraceLevel, orclTraceMode, orclUserDN, orclWriteWaitThreads

**Object Classes**

orclGeneralStats, orclHealthStats, orclPerfStats, orclSecRefreshEvents, orclSM, orclTraceConfig, orclUserStats

## 6.2.5 Oracle Directory Replication Schema Elements

This section lists the schema elements for directory replication.

**Attributes**

orclAgreementId, orclChangeLogLife, orclChangeRetryCount, orclCompatibleVersion, orclDirReplGroupAgreement, orclDirReplGroupDSAs, orclExcludedAttributes, orclExcludedNamingContexts, orclHIQSchedule, orclHostname, orclIncludedNamingContexts, orclLastAppliedChangeNumber, orclLDAPConnKeepAlive, orclPilotMode, orclPurgeSchedule, orclReplicaDN, orclReplicaID, orclReplicaSecondaryURI, orclReplicaState, orclReplicationProtocol, orclReplicaType, orclReplicaURI, orclReplicaVersion, orclThreadsPerSupplier, orclUpdateSchedule, pilotStartTime

**Object Classes**

orclReplAgreementEntry, orclReplInstance, orclReplicaSubentry, orclReplNameCtxConfig, orclReplSubConfig

## 6.2.6 Oracle Directory Integration and Provisioning Schema Elements

This section lists the schema elements for Oracle Directory Integration and Provisioning. It contains the following topics:

- Section 6.2.6.1, "Applications"
- Section 6.2.6.2, "Change Logs"
- Section 6.2.6.3, "Events and Objects"
- Section 6.2.6.4, "Plug-ins and Interfaces"
- Section 6.2.6.5, "Server Configuration"
- Section 6.2.6.6, "Profiles"
- Section 6.2.6.7, "Schema"
- Section 6.2.6.8, "Active Directory Users"

### 6.2.6.1 Applications

This section lists the attributes and object classes for Oracle Directory Integration and Provisioning applications.

#### Attributes

orclApplicationType, orclInterval, orclODIPAgent, orclODIPApplicationName, orclODIPCommand, orclODIPDbConnectInfo, orclODIPEventSubscriptions, orclOwnerGUID, orclStatus, orclVersion

#### Object Classes

orclODIPApplicationCommonConfig, orclODIPAppSubscription

### 6.2.6.2 Change Logs

This section lists the attributes and object classes for Oracle Directory Integration and Provisioning change logs.

#### Attributes

orclLastAppliedChangeNumber, orclSubscriberDisable, serverName, userPassword

#### Object Classes

orclChangeSubscriber

### 6.2.6.3 Events and Objects

This section lists the attributes and object classes for Oracle Directory Integration and Provisioning events and objects.

#### Attributes

orclODIPAttributeMappingRules, orclODIPEventFilter, orclODIPFilterAttrCriteria, orclODIPMustAttrCriteria, orclODIPObjectCriteria, orclODIPObjectEvents, orclODIPObjectName, orclODIPObjectSyncBase, orclODIPOperationMode, orclODIPOptAttrCriteria, orclODIPProvEventCriteria, orclODIPProvEventLDAPChangeType, orclODIPProvEventObjectType, orclODIPProvEventRule, orclODIPProvEventRuleDTD, orclStatus

### Object Classes

orclODIPEventContainer, orclODIPObject, orclODIPProvEventDefn, orclODIPProvEventTypeConfig

#### 6.2.6.4 Plug-ins and Interfaces

This section lists the attributes and object classes for Oracle Directory Integration and Provisioning plug-ins and interfaces.

### Attributes

orclODIPPluginAddInfo, orclODIPPluginConfigInfo, orclODIPPluginEvents, orclODIPPluginExecData, orclODIPPluginExecName, orclODIPProfileProvSubscriptionMode, orclODIPProfileStatusUpdate, orclODIPProvInterfaceFilter, orclODIPProfileInterfaceType, orclODIPProvInterfaceProcessor, orclStatus

### Object Classes

orclODIPProvInterfaceDetails, orclODIPPlugin, orclODIPPluginContainer

#### 6.2.6.5 Server Configuration

This section lists the attributes and object classes for configuring the Oracle Directory Integration and Provisioning server.

### Attributes

cn, orclCompatibleVersion, orclHostname, orclODIPConfigDNs, orclODIPConfigRefreshFlag, orclODIPInstanceStatus, orclODIPProfileExecGroupID, orclODIPSearchCountLimit, orclODIPSearchTimeLimit, orclODIPServerCommitSize, orclODIPServerDebugLevel, orclODIPServerRefreshIntvl, orclODIPServerSSLMode, orclODIPServerWalletLoc, orclSSLEnable, orclVersion, seeAlso, userPassword

### Object Classes

orclODIPServerConfig, orclODISConfig, orclODIServer, orclODISInstance

#### 6.2.6.6 Profiles

This section the attributes and object classes for Oracle Directory Integration and Provisioning synchronization and provisioning profiles.

### Attributes

cn, orclODIPAgentConfigInfo, orclODIPAgentControl, orclODIPAgentExeCommand, orclODIPAgentHostName, orclODIPAgentName, orclODIPAgentPassword, orclODIPAttributeMappingRules, orclODIPBootStrapStatus, orclODIPConDirAccessAccount, orclODIPConDirAccessPassword, orclODIPConDirLastAppliedChgNum, orclODIPConDirMatchingFilter, orclODIPConDirURL, orclODIPEncryptedAttrKey, orclODIPInterfaceType, orclODIPLastExecutionTime, orclODIPLastSuccessfulExecutionTime, orclODIPOIDMatchingFilter, orclODIPProfileDebugLevel, orclODIPProfileExecGroupID, orclODIPProfileInterfaceAdditionalInformation, orclODIPProfileInterfaceConnectInformation, orclODIPProfileInterfaceName, orclODIPProfileInterfaceType, orclODIPProfileInterfaceVersion, orclODIPProfileLastAppliedAppEventID, orclODIPProfileLastProcessingTime, orclODIPProfileLastSuccessfulProcessingTime, orclODIPProfileMaxErrors, orclODIPProfileMaxEventsPerInvocation, orclODIPProfileMaxEventsPerSchedule, orclODIPProfileMaxRetries, orclODIPProfileName, orclODIPProfileProcessingErrors,



orclODIPProfileProcessingStatus, orclODIPProfileSchedule,  
 orclODIPProvisioningAppGUID, orclODIPProvisioningAppName,  
 orclODIPProvisioningEventMappingRules,  
 orclODIPProvisioningEventPermittedOperations,  
 orclODIPProvisioningEventSubscription, orclODIPProvisioningOrgGUID,  
 orclODIPProvisioningOrgName, orclODIPSchedulingInterval,  
 orclODIPSynchronizationErrors, orclODIPSynchronizationMode,  
 orclODIPSynchronizationStatus, orclODIPSyncRetryCount, orclPasswordAttribute,  
 orclStatus, orclVersion, userPassword

### Object Classes

orclODIPIntegrationProfile, orclODIPProfile, orclODIPProvisioningIntegrationProfile,  
 orclODIPProvisioningIntegrationProfileV2,  
 orclODIPProvisioningIntegrationOutBoundProfile,  
 orclODIPProvisioningIntegrationOutBoundProfileV2

### 6.2.6.7 Schema

This section lists the attributes and object classes for Oracle Directory Integration and Provisioning schema information.

#### Attributes

orclODIPApplicationsLocation, orclODIPInstancesLocation,  
 orclODIPObjectDefnLocation, orclODIPProvProfileLocation, orclODIPRootLocation,  
 orclODIPSchemaVersion, orclODIPServerConfigLocation,  
 orclODIPSyncProfileLocation

#### Object Classes

orclODIPSchemaDetails

### 6.2.6.8 Active Directory Users

The following attributes and object classes are used for users that are imported into Oracle Internet Directory from Microsoft Active Directory using Oracle Directory Integration and Provisioning.

#### Attributes

orclObjectGUID, orclObjectSID, orclSAMAccountName, orclUserPrincipalName

#### Object Classes

orclADGroup, orclADUser, orclNTUser

## 6.2.7 Oracle Delegated Administration Services Schema Elements

This section lists the attributes and object classes for Oracle Delegated Administration Services.

#### Attributes

orclDASAdminModifiable, orclDASAttrDispOrder, orclDASAttrName,  
 orclDASEnableProductLogo, orclDASEnableSubscriberLogo, orclDASIsEnabled,  
 orclDASIsMandatory, orclDASIsPersonal, orclDASLOV, orclDASPublicGroupDNs,  
 orclDASSearchable, orclDASSearchColIndex, orclDASSearchFilter,  
 orclDASSearchSizeLimit, orclDASSelfModifiable, orclDASUIType, orclDASURL,  
 orclDASURLBase, orclDASValidatePwdReset, orclDASViewable

### **Object Classes**

orclDASAppContainer, orclDASAttrCategory, orclDASConfigAttr,  
orclDASConfigPublicGroup, orclDASLOVVal, orclDASOperationURL,  
orclDASSubscriberContainer

## **6.2.8 Oracle Application Server Certificate Authority and PKI Schema Elements**

This section lists the attributes and object classes that pertain to public key infrastructure (PKI), certificates, and Oracle Application Server Certificate Authority.

### **Attributes**

orclCertExtensionAttribute, orclCertExtensionOID, orclCertificateHash,  
orclCertificateMatch, orclCertMappingAttribute, orclPKINextUpdate,  
orclPKIValMecAttr, x509issuer

### **Object Classes**

orclCertIdMapping, orclPKICRL, orclPKIValMecCl

## **6.2.9 Application Schema Elements**

This section lists the attributes and object classes that pertain to applications.

### **Attributes**

authPassword, description, labeledURI, orclAppFullName,  
orclApplicationCommonName, orclCategory, orclDBSchemaIdentifier,  
orclOwnerGUID, orclPasswordVerifier, orclResourceIdentifier,  
orclTrustedApplicationGroup, orclVersion, protocolInformation, seeAlso,  
userCertificate;binary, userPassword, userPKCS12

### **Object Classes**

orclApplicationEntity, orclAppSpecificUserInfo, orclAppUserEntry

## **6.2.10 Resource Schema Elements**

This section lists the attributes and object classes that pertain to resources.

### **Attributes**

description, displayName, javaClassName, orclConnectionFormat, orclFlexAttribute1,  
orclFlexAttribute2, orclFlexAttribute3, orclOwnerGUID, orclPasswordAttribute,  
orclResourceName, orclResourceTypeName, orclResourceViewers,  
orclUserIDAttribute, orclUserModifiable

### **Object Classes**

orclResourceDescriptor, orclResourceType

## **6.2.11 Plug-in Schema Elements**

This section lists the attributes and object classes for configuring Plug-ins for Oracle Internet Directory.

### **Attributes**

orclPluginAttributeList, orclPluginCheckEntryExist, orclPluginEnable,  
orclPluginEntryProperties, orclPluginIsReplace, orclPluginKind,

orclPluginLDAPOperation, orclPluginName, orclPluginPort, orclPluginRequestGroup, orclPluginRequestNegGroup, orclPluginResultCode, orclPluginSASLCallBack, orclPluginSearchNotFound, orclPluginShareLibLocation, orclPluginSubscriberDNList, orclPluginTiming, orclPluginType, orclPluginVersion, userPassword

### Object Classes

orclPluginConfig, orclPluginContainer, orclPluginUser

## 6.2.12 Directory User Agents Schema Elements

This section lists the attributes and object classes for configuring directory user agents (DUAs).

### Attributes

attributeMap, authenticationMethod, bindTimeLimit, cn, credentialLevel, defaultSearchBase, defaultSearchScope, defaultServerList, followReferrals, objectClass, objectClassMap, preferredServerList, profileTTL, serviceAuthenticationMethod, serviceCredentialLevel, serviceSearchDescriptor

### Object Classes

duaConfigProfile

## 6.2.13 User, Group, and Subscriber Schema Elements

This section lists the attributes and object classes used for users, groups, and subscribers. It contains the following topics:

- Section 6.2.13.1, "Groups"
- Section 6.2.13.2, "Dynamic Groups"
- Section 6.2.13.3, "Users"

### 6.2.13.1 Groups

Oracle Internet Directory uses the standard object classes `groupOfNames` and `groupOfUniqueNames` as defined in RFC 2256. In addition to the standard attributes and object classes, the following are also used for groups.

### Attributes

displayName, mail, orclGlobalID, orclIsVisible

### Object Classes

orclGroup

### 6.2.13.2 Dynamic Groups

This section lists the attributes and object classes for dynamic groups.

### Attributes

labeledURI, mail, orclConnectByAttribute, orclConnectBySearchBase, orclConnectByStartingValue

### Object Classes

orclDynamicGroup

### 6.2.13.3 Users

Oracle Internet Directory uses the standard object classes `person` and `inetOrgPerson` as defined in RFC 2256. In addition to the standard attributes and object classes, the following are also used for users.

#### Attributes

`authPassword`, `c`, `jpegPhoto`, `krbPrincipalName`, `middleName`, `orclActiveEndDate`, `orclActiveStartDate`, `orclContact`, `orclDateOfBirth`, `orclDefaultProfileGroup`, `orclDisplayPersonalInfo`, `orclGender`, `orclHireDate`, `orclHostedCreditCardExpireDate`, `orclHostedCreditCardNumber`, `orclHostedCreditCardType`, `orclHostedDunsNumber`, `orclHostedPaymentTerm`, `orclIsEnabled`, `orclIsVisible`, `orclMaidenName`, `orclPassword`, `orclPasswordHint`, `orclPasswordHintAnswer`, `orclPasswordVerifier`, `orclPKCS12Hint`, `orclSAMAccountName`, `orclSearchFilter`, `orclSubscriberFullName`, `orclSubscriberType`, `orclTimeZone`, `orclTxnMaxOperations`, `orclVersion`, `orclWirelessAccountNumber`, `orclWorkflowNotificationPref`, `userPKCS12`

#### Object Classes

`orclSubscriber`, `orclUserV2`

## 6.2.14 Password Policy Schema Elements

This section lists the attributes and object classes that pertain to password policy configuration.

#### Attributes

`cn`, `displayName`, `orclPwdAllowHashCompare`, `orclPwdAlphaNumeric`, `orclPwdEncryptionEnable`, `orclPwdIllegalValues`, `orclPwdIPLockout`, `orclPwdIPLockoutDuration`, `orclPwdIPMaxFailure`, `orclPwdPolicyEnable`, `pwdAllowUserChange`, `pwdCheckSyntax`, `pwdExpireWarning`, `pwdFailureCountInterval`, `pwdGraceLoginLimit`, `pwdInHistory`, `pwdLockout`, `pwdLockoutDuration`, `pwdMaxAge`, `pwdMaxFailure`, `pwdMinAge`, `pwdMinLength`, `pwdMustChange`, `pwdSafeModify`

#### Object Classes

`pwdpolicy`

## 6.2.15 Password Verifier Schema Elements

This section lists the attributes and object classes that pertain to password verifiers.

#### Attributes

`cn`, `displayName`, `orclAppId`, `orclPwdVerifierParams`, `owner`

#### Object Classes

`orclPwdVerifierProfile`

---



---

## LDAP Object Class Reference

This chapter provides reference information about the object classes used for Oracle Identity Management.

This chapter includes the following sections:

- Section 7.1, "Standard LDAP Object Classes"
- Section 7.2, "Oracle Identity Management Object Class Reference"

For a list of object classes grouped by functional categories, see Section 6.2, "Overview of Oracle Identity Management Schema Elements."

### 7.1 Standard LDAP Object Classes

Oracle Internet Directory supports the following standard LDAP object classes as defined in the Internet Engineering Task Force (IETF) Requests for Comments (RFC) specifications.

Details of RFC specifications can be found on the IETF Web site at:  
<http://www.ietf.org>.

**Table 7-1 Standard LDAP Object Classes Used By Oracle Internet Directory**

Object Class Name	Specification
accessControlSubentry	RFC 1274
account	RFC 1274
alias	RFC 2256
applicationEntity	RFC 2256
applicationProcess	RFC 2256
bootableDevice	RFC 2307
certificationAuthority	RFC 2256
certificationAuthority-V2	RFC 2256
collectiveAttributeSubentry	RFC 3671
country	RFC 2256
crlDistributionPoint	RFC 2256
device	RFC 2256
dmd	RFC 2256
dnsDomain	RFC 1274

**Table 7-1 (Cont.) Standard LDAP Object Classes Used By Oracle Internet Directory**

<b>Object Class Name</b>	<b>Specification</b>
documentSeries	RFC 1274
domain	RFC 1274
domainRelatedObject	RFC 1274
dsa	RFC 1274
extensibleObject	RFC 2252
friendlyCountry	RFC 1274
groupOfNames	RFC 2256
groupOfUniqueNames	RFC 2256
ieee802Device	RFC 2307
inetOrgPerson	RFC 2798
ipHost	RFC 2307
ipNetwork	RFC 2307
ipProtocol	RFC 2307
ipService	RFC 2307
javaContainer	RFC 2713
javaMarshaledObject	RFC 2713
javaNamingReference	RFC 2713
javaObject	RFC 2713
javaSerializedObject	RFC 2713
labeledURIObject	RFC 2079
locality	RFC 2256
newPilotPerson	RFC 2377
nisDomainObject	RFC 2307
nisKeyObject	RFC 2307
nisMap	RFC 2307
nisNetgroup	RFC 2307
nisObject	RFC 2307
oldQualityLabelledData	RFC 2307
oncRpc	RFC 2307
organization	RFC 2256
organizationalPerson	RFC 2256
organizationalRole	RFC 2256
organizationalUnit	RFC 2256
person	RFC 2256
pilotDSA	RFC 2256
pilotObject	RFC 2256
pilotOrganization	RFC 2256

**Table 7–1 (Cont.) Standard LDAP Object Classes Used By Oracle Internet Directory**

Object Class Name	Specification
posixAccount	RFC 2307
posixGroup	RFC 2307
referral	RFC 3296
residentialPerson	RFC 2256
room	RFC 1274
shadowAccount	RFC 2307
simpleSecurityObject	RFC 1274
strongAuthenticationUser	RFC 2256

## 7.2 Oracle Identity Management Object Class Reference

This section contains an alphabetical listing of the Oracle Identity Management object classes. These are the object classes used to create entries pertaining to Oracle Internet Directory, Oracle Directory Integration and Provisioning, Oracle Delegated Administration Services, Oracle Single Sign-On, and Oracle Application Server Certificate Authority. For more information about an attribute or the superior of an object class, click the link of the attribute name or superior object class name.

### 7.2.1 `duaConfigProfile`

#### Description

Configuration profile for a directory user agent (DUA). A DUA is software that accesses the LDAP directory service on behalf of the directory user. The directory user may be a person or another software element.

#### Object ID

1.3.6.1.4.1.11.1.3.1.2.4

#### Superior Object Class

[top](#)

#### Object Class Type

88

#### Required Attributes

[cn](#), [objectClass](#)

#### Allowed Attributes

[attributeMap](#), [authenticationMethod](#), [bindTimeLimit](#), [credentialLevel](#), [defaultSearchBase](#), [defaultSearchScope](#), [defaultServerList](#), [followReferrals](#), [objectClassMap](#), [preferredServerList](#), [profileTTL](#), [serviceAuthenticationMethod](#), [serviceCredentialLevel](#), [serviceSearchDescriptor](#)

## 7.2.2 orclADGroup

**Description**

Contains Microsoft Active Directory group attributes, which are used to synchronize Active Directory group objects with Oracle Internet Directory group objects in an Oracle Directory Integration and Provisioning environment.

**Object ID**

2.16.840.1.113894.8.2.899

**Superior Object Class**

[top](#)

**Object Class Type**

Structural

**Required Attributes**

[orclSAMAccountName](#)

**Allowed Attributes**

[displayName](#), [orclObjectGUID](#), [orclObjectSID](#)

## 7.2.3 orclADUser

**Description**

Contains Microsoft Active Directory user attributes, which are used to synchronize Active Directory user objects with Oracle Internet Directory user objects in an Oracle Directory Integration and Provisioning environment.

**Object ID**

2.16.840.1.113894.8.2.900

**Superior Object Class**

[top](#)

**Object Class Type**

Structural

**Required Attributes**

[orclSAMAccountName](#)

**Allowed Attributes**

[displayName](#), [orclObjectGUID](#), [orclObjectSID](#), [orclUserPrincipalName](#)

## 7.2.4 orclApplicationEntity

**Description**

Defines an application entity.



**Object ID**

2.16.840.1.113894.1.2.55

**Superior Object Class**[top](#)**Object Class Type**

Structural

**Required Attributes**

N/A

**Allowed Attributes**

[authPassword](#), [description](#), [labeledURI](#), [orclAppFullName](#), [orclApplicationAddress](#), [orclApplicationCommonName](#), [orclCategory](#), [orclDBSchemaIdentifier](#), [orclPasswordVerifier](#), [orclResourceIdentifier](#), [orclTrustedApplicationGroup](#), [orclVersion](#), [protocolInformation](#), [seeAlso](#), [userCertificate;binary](#), [userPassword](#), [userPKCS12](#)

## 7.2.5 orclAppSpecificUserInfo

**Description**

An auxiliary object class for an application entity that defines user information.

**Object ID**

2.16.840.1.13894.8.2.420

**Superior Object Class**[top](#)**Object Class Type**

Auxilliary

**Required Attributes**[orclOwnerGUID](#)**Allowed Attributes**

N/A

## 7.2.6 orclAppUserEntry

**Description**

The user associated with an application entity.

**Object ID**

2.16.840.1.13894.8.2.423

**Superior Object Class**[top](#)

**Object Class Type**

Structural

**Required Attributes**

[orclOwnerGUID](#)

**Allowed Attributes**

N/A

## 7.2.7 orclAuditOC

**Description**

Generic audit log attributes that can be used in a server audit log entry.

**Object ID**

2.16.840.1.113894.1.2.18

**Superior Object Class**

[top](#)

**Object Class Type**

Structural

**Required Attributes**

[orclAuditMessage](#), [orclEventTime](#), [orclEventType](#), [orclSequence](#)

**Allowed Attributes**

[orclAuditAttribute](#), [orclOpResult](#), [orclUserDN](#)

## 7.2.8 orclCertIdMapping

**Description**

Oracle Internet Directory public key infrastructure (PKI) structural object class for mapping attributes in a client certificate to entries in Oracle Internet Directory.

**Object ID**

2.16.840.1.113894.1.2.130

**Superior Object Class**

[top](#)

**Object Class Type**

Structural

**Required Attributes**

[cn](#)

**Allowed Attributes**

[description](#), [orclCertExtensionAttribute](#), [orclCertExtensionOID](#),  
[orclCertMappingAttribute](#)

## 7.2.9 orclChangeSubscriber

**Description**

Status information for an Oracle Directory Integration and Provisioning change subscriber event.

**Object ID**

2.16.840.1.113894.1.2.21

**Superior Object Class**

[top](#)

**Object Class Type**

Structural

**Required Attributes**

[orclLastAppliedChangeNumber](#), [orclSubscriberDisable](#)

**Allowed Attributes**

[cn](#), [serverName](#), [userPassword](#)

## 7.2.10 orclCommonAttributes

**Description**

Oracle Context configuration attributes.

**Object ID**

2.16.840.1.113894.7.2.1004

**Superior Object Class**

[orclContainer](#)

**Object Class Type**

Structural

**Required Attributes**

N/A

**Allowed Attributes**

[orclCommonAutoRegEnabled](#), [orclCommonContextMap](#),  
[orclCommonDefaultUserCreateBase](#), [orclCommonGroupCreateBase](#),  
[orclCommonNamingAttribute](#), [orclCommonNicknameAttribute](#),  
[orclCommonSASLRealm](#), [orclCommonUserSearchBase](#), [orclVersion](#)

## 7.2.11 orclCommonAttributesV2

### Description

Oracle Context configuration attributes.

### Object ID

2.16.840.1.113894.1.2.51

### Superior Object Class

[top](#)

### Object Class Type

88

### Required Attributes

N/A

### Allowed Attributes

[orclDefaultSubscriber](#), [orclSubscriberNickNameAttribute](#), [orclSubscriberSearchBase](#), [orclUserObjectClasses](#)

## 7.2.12 orclConfigSet

### Description

Configuration set entry for a server instance.

### Object ID

2.16.840.1.113894.1.2.2

### Superior Object Class

[top](#)

### Object Class Type

Structural

### Required Attributes

[cn](#)

### Allowed Attributes

[description](#), [seeAlso](#)

## 7.2.13 orclContainer

### Description

Container object for an Oracle Context.

### Object ID

2.16.840.1.113894.7.2.2

**Superior Object Class**[top](#)**Object Class Type**

Structural

**Required Attributes**[cn](#)**Allowed Attributes**[orclVersion](#), [orclServiceType](#)

## 7.2.14 orclDASAppContainer

**Description**

Container object for a Oracle Delegated Administration Services application.

**Object ID**

2.16.840.1.113894.1.2.61

**Superior Object Class**[top](#)**Object Class Type**

Auxilliary

**Required Attributes**

N/A

**Allowed Attributes**[orclDASURLBase](#)

## 7.2.15 orclDASAttrCategory

**Description**

Oracle Delegated Administration Services attribute categories.

**Object ID**

2.16.840.1.113894.1.2.59

**Superior Object Class**

N/A

**Object Class Type**

Auxilliary

**Required Attributes**

N/A

**Allowed Attributes**

[cn](#), [displayName](#), [orclDASAttrDispOrder](#), [orclDASAttrName](#)

## 7.2.16 orclDASConfigAttr

**Description**

Oracle Delegated Administration Services configuration attributes.

**Object ID**

2.16.840.1.113894.1.2.56

**Superior Object Class**

[top](#)

**Object Class Type**

Auxilliary

**Required Attributes**

N/A

**Allowed Attributes**

[displayName](#), [orclDASAdminModifiable](#), [orclDASIsMandatory](#), [orclDASIsPersonal](#), [orclDASLOV](#), [orclDASSearchable](#), [orclDASSearchColIndex](#), [orclDASSearchFilter](#), [orclDASSelfModifiable](#), [orclDASUIType](#), [orclDASValidatePwdReset](#), [orclDASViewable](#)

## 7.2.17 orclDASConfigPublicGroup

**Description**

Oracle Delegated Administration Services public group configuration attributes.

**Object ID**

2.16.840.1.113894.1.2.60

**Superior Object Class**

[top](#)

**Object Class Type**

Auxilliary

**Required Attributes**

[cn](#)

**Allowed Attributes**

[orclDASIsEnabled](#), [orclDASPublicGroupDNs](#)

## 7.2.18 orclDASLOVVal

**Description**

Oracle Delegated Administration Services list of values.

**Object ID**

2.16.840.1.113894.1.1.919

**Superior Object Class**[top](#)**Object Class Type**

Structural

**Required Attributes**[cn](#), [displayName](#)**Allowed Attributes**

N/A

## 7.2.19 orclDASOperationURL

**Description**

Oracle Delegated Administration Services URL.

**Object ID**

2.16.840.1.113894.1.2.54

**Superior Object Class**[top](#)**Object Class Type**

Auxilliary

**Required Attributes**

N/A

**Allowed Attributes**[cn](#), [description](#), [orclDASURL](#)

## 7.2.20 orclDASSubscriberContainer

**Description**

Oracle Delegated Administration Services subscriber container object.

**Object ID**

2.16.840.1.113894.1.2.66

**Superior Object Class**

N/A

**Object Class Type**

Structural

**Required Attributes**

N/A

**Allowed Attributes**

[orclDASEnableProductLogo](#), [orclDASEnableSubscriberLogo](#), [orclDASSearchSizeLimit](#)

## 7.2.21 orclIDMapping

**Description**

Auxilliary object class defining the attributes that hold information about directory operations to be performed for mapping.

**Object ID**

2.16.840.1.113894.1.2.131

**Superior Object Class**

[top](#)

**Object Class Type**

Auxilliary

**Required Attributes**

N/A

**Allowed Attributes**

[orclMappedDN](#), [orclSearchBaseDN](#), [orclSearchFilter](#), [orclSearchScope](#)

## 7.2.22 orclDSAConfig

**Description**

Configuration attributes for Oracle Internet Directory server.

**Object ID**

2.16.840.1.113894.1.2.70

**Superior Object Class**

[top](#)

**Object Class Type**

Structural

**Required Attributes**

[cn](#)

**Allowed Attributes**

[orclAnonymousBindsFlag](#), [orclCatalogEntryDN](#), [orclCryptoScheme](#), [orclDebugFlag](#), [orclDebugForceFlush](#), [orclDebugOp](#), [orclDIPRepository](#), [orclEcacheEnabled](#), [orclEcacheMaxEntries](#), [orclEcacheMaxSize](#), [orclEnableGroupCache](#), [orclGUPassword](#), [orclIpAddress](#), [orclLDAPConnTimeout](#), [orclMatchDnEnabled](#), [orclMaxConnInCache](#),



orclNwrwTimeout, orclPKIMatchingRule, orclPrName, orclPrPassword,  
 orclReplAgreements, orclReplicaID, orclsDumpFlag, orclServerMode, orclSizeLimit,  
 orclSkewedAttribute, orclSkipRefInSQL, orclStatsDN, orclStatsFlag, orclStatsLevel,  
 orclStatsOp, orclStatsPeriodicity, orclSUAccountLocked, orclSULoginFailureCount,  
 orclSUName, orclSUPassword, orclTimeLimit, orclTLimitMode,  
 orclUpgradeInProgress

## 7.2.23 orclDynamicGroup

### Description

Object class that is used to create dynamic groups. A dynamic group is one whose membership, rather than being maintained in a list, is computed on the fly, based on rules and assertions you specify. In the case of `orclDynamicGroup` using `labeleduri` attribute, the members of the list are cached.

### Object ID

2.16.840.1.113894.1.2.190

### Superior Object Class

N/A

### Object Class Type

Auxilliary

### Required Attributes

N/A

### Allowed Attributes

`labeledURI`, `mail`, `orclConnectByAttribute`, `orclConnectBySearchBase`,  
`orclConnectByStartingValue`

## 7.2.24 orclDynamicList

### Description

Objectclass that is used to create dynamic groups. A dynamic group is one whose membership, rather than being maintained in a list, is computed on the fly, based on rules and assertions you specify. In the case of `orclDynamicList`, members are not cached.

### Object ID

2.16.840.1.113894.1.1.425

### Superior Object Class

N/A

### Object Class Type

Auxilliary

### Required Attributes

`labeledURI`

**Allowed Attributes**

N/A

## 7.2.25 orclEventLog

**Description**

Object class used for audit logging of server events.

**Object ID**

2.16.840.1.113894.1.2.17

**Superior Object Class**

[top](#)

**Object Class Type**

Structural

**Required Attributes**

[cn](#)

**Allowed Attributes**

## 7.2.26 orclEvents

**Description**

Object class used for audit logging of events.

**Object ID**

2.16.840.1.113894.1.2.19

**Superior Object Class**

[top](#)

**Object Class Type**

Structural

**Required Attributes**

[cn](#)

**Allowed Attributes**

[orclEventType](#)

## 7.2.27 orclGeneralStats

**Description**

Statistical information for Oracle Internet Directory server operations.

**Object ID**

2.16.840.1.113894.1.2.30

**Superior Object Class**

N/A

**Object Class Type**

Auxilliary

**Required Attributes**

N/A

**Allowed Attributes**[orclOpAbandoned](#), [orclOpCompleted](#), [orclOpInitiated](#), [orclOpPending](#), [orclOpTimedOut](#), [orclQueueDepth](#)

## 7.2.28 orclGroup

**Description**

Additional optional attributes for a group.

**Object ID**

2.16.840.1.113894.1.2.53

**Superior Object Class**[top](#)**Object Class Type**

Auxilliary

**Required Attributes**

N/A

**Allowed Attributes**[displayName](#), [mail](#), [orclGlobalID](#), [orclIsVisible](#)

## 7.2.29 orclHealthStats

**Description**

Statistical information for Oracle Internet Directory server performance.

**Object ID**

2.16.840.1.113894.1.2.27

**Superior Object Class**

N/A

**Object Class Type**

Auxilliary

**Required Attributes**

N/A

**Allowed Attributes**

[orclActiveThreads](#), [orclEcacheHitRatio](#), [orclEcacheNumEntries](#), [orclEcacheSize](#), [orclIdleConn](#), [orclIdleThreads](#), [orclInitialServerMemSize](#), [orclOpenConn](#), [orclQueueDepth](#), [orclQueueLatency](#), [orclReadWaitThreads](#), [orclServerAvgMemGrowth](#), [orclTcpConnToClose](#), [orclTcpConnToShutDown](#), [orclTotFreePhyMem](#), [orclWriteWaitThreads](#)

## 7.2.30 orclIndexOC

**Description**

Configuration of the indexed attributes for the Oracle Internet Directory server.

**Object ID**

2.16.840.1.113894.1.2.15

**Superior Object Class**

[top](#)

**Object Class Type**

Structural

**Required Attributes**

[cn](#)

**Allowed Attributes**

[orclIndexedAttribute](#)

## 7.2.31 orclLDAPInstance

**Description**

Configuration attributes for an Oracle Internet Directory server instance.

**Object ID**

2.16.840.1.113894.1.2.13

**Superior Object Class**

[top](#), [orclLDAPSubConfig](#)

**Object Class Type**

Structural

**Required Attributes**

[cn](#), [orclCompatibleVersion](#), [orclHostname](#)

**Allowed Attributes**

[description](#), [seeAlso](#)

## 7.2.32 orclLDAPSubConfig

**Description**

Configuration attributes for Oracle Internet Directory server.

**Object ID**

2.16.840.1.113894.1.2.3

**Superior Object Class**

[top](#), [orclConfigSet](#)

**Object Class Type**

Structural

**Required Attributes**

[cn](#)

**Allowed Attributes**

[orclMaxCC](#), [orclNonSSLPort](#), [orclSASLAuthenticationMode](#), [orclSASLCipherChoice](#), [orclSASLMechanism](#), [orclServerProcs](#), [orclSSLAuthentication](#), [orclSSLCipherSuite](#), [orclSSLEnable](#), [orclSSLPort](#), [orclSSLVersion](#), [orclSSLWalletURL](#)

## 7.2.33 orclNTUser

**Description**

Contains Microsoft NT user attributes, which are used to synchronize NT user objects with Oracle Internet Directory user objects in an Oracle Directory Integration and Provisioning environment.

**Object ID**

2.16.840.1.113894.8.2.898

**Superior Object Class**

[top](#)

**Object Class Type**

Structural

**Required Attributes**

[orclSAMAccountName](#)

**Allowed Attributes**

[displayName](#), [orclObjectGUID](#), [orclObjectSID](#)

## 7.2.34 orclODIPApplicationCommonConfig

**Description**

Oracle Directory Integration and Provisioning configuration attributes.

**Object ID**

2.16.840.1.13894.8.2.421

**Superior Object Class**

[top](#)

**Object Class Type**

Auxilliary

**Required Attributes**

N/A

**Allowed Attributes**

[orclApplicationType](#)

## 7.2.35 orclODIPAppSubscription

**Description**

Application subscription attributes for Oracle Directory Integration and Provisioning.

**Object ID**

2.16.840.1.113894.9.2.1

**Superior Object Class**

[top](#)

**Object Class Type**

Structural

**Required Attributes**

N/A

**Allowed Attributes**

[orclInterval](#), [orclODIPAgent](#), [orclODIPApplicationName](#), [orclODIPCommand](#), [orclODIPDbConnectInfo](#), [orclODIPEventSubscriptions](#), [orclOwnerGUID](#), [orclStatus](#), [orclVersion](#)

## 7.2.36 orclODIPEventContainer

**Description**

Container object for an Oracle Directory Integration and Provisioning event.

**Object ID**

2.16.840.1.113894.8.2.414

**Superior Object Class**

N/A

**Object Class Type**

88

**Required Attributes**[cn](#)**Allowed Attributes**[orclODIPAttributeMappingRules](#), [orclODIPEventFilter](#), [orclODIPOperationMode](#), [orclODIPProvEventRule](#), [orclStatus](#)

## 7.2.37 orclODIPIntegrationProfile

**Description**

Oracle Directory Integration and Provisioning integration profiles for integrating with third-party directories.

**Object ID**

2.16.840.1.113894.8.2.200

**Superior Object Class**[top](#)**Object Class Type**

Structural

**Required Attributes**[orclODIPProfileName](#), [orclVersion](#)**Allowed Attributes**[orclODIPEncryptedAttrKey](#), [orclODIPProfileDebugLevel](#), [orclODIPProfileExecGroupID](#), [orclODIPProfileInterfaceAdditionalInformation](#), [orclODIPProfileInterfaceConnectInformation](#), [orclODIPProfileInterfaceName](#), [orclODIPProfileInterfaceType](#), [orclODIPProfileInterfaceVersion](#), [orclODIPProfileLastProcessingTime](#), [orclODIPProfileLastSuccessfulProcessingTime](#), [orclODIPProfileMaxErrors](#), [orclODIPProfileMaxEventsPerInvocation](#), [orclODIPProfileMaxEventsPerSchedule](#), [orclODIPProfileMaxRetries](#), [orclODIPProfileProcessingErrors](#), [orclODIPProfileProcessingStatus](#), [orclODIPProfileSchedule](#), [orclPasswordAttribute](#), [orclStatus](#), [userPassword](#)

## 7.2.38 orclODIPObject

**Description**

Attributes to identify Oracle Directory Integration and Provisioning objects.

**Object ID**

2.16.840.1.113894.8.2.431

**Superior Object Class**[top](#)

**Object Class Type**

Auxilliary

**Required Attributes**

[orclODIPObjectCriteria](#), [orclODIPObjectName](#)

**Allowed Attributes**

[orclODIPFilterAttrCriteria](#), [orclODIPMustAttrCriteria](#), [orclODIPOptAttrCriteria](#)

## 7.2.39 orclODIPPlugin

**Description**

Configuration attributes for Oracle Directory Integration and Provisioning plug-ins.

**Object ID**

2.16.840.1.113894.8.2.412

**Superior Object Class**

N/A

**Object Class Type**

Structural

**Required Attributes**

[cn](#), [orclODIPPluginEvents](#), [orclODIPPluginExecName](#)

**Allowed Attributes**

[description](#), [orclODIPPluginAddInfo](#), [orclStatus](#)

## 7.2.40 orclODIPPluginContainer

**Description**

Configuration attributes for Oracle Directory Integration and Provisioning plug-ins.

**Object ID**

2.16.840.1.113894.8.2.411

**Superior Object Class**

N/A

**Object Class Type**

Structural

**Required Attributes**

[cn](#)

**Allowed Attributes**

[description](#), [orclODIPPluginConfigInfo](#), [orclODIPPluginExecData](#)



## 7.2.41 orclODIPProvEventDefn

**Description**

Defines a provisioning event.

**Object ID**

2.16.840.1.113894.8.2.413

**Superior Object Class**

N/A

**Object Class Type**

88

**Required Attributes**

N/A

**Allowed Attributes**

[cn](#), [orclODIPEventFilter](#), [orclODIPObjectEvents](#), [orclODIPObjectName](#), [orclODIPObjectSyncBase](#), [orclODIPProvEventRule](#), [orclStatus](#)

## 7.2.42 orclODIPProvEventTypeConfig

**Description**

Configuration attributes for a provisioning event type.

**Object ID**

2.16.840.1.113894.8.2.500

**Superior Object Class**

[top](#)

**Object Class Type**

Structural

**Required Attributes**

[orclODIPProvEventObjectType](#)

**Allowed Attributes**

[orclODIPProvEventCriteria](#), [orclODIPProvEventLDAPChangeType](#)

## 7.2.43 orclODIPProvInterfaceDetails

**Description**

Provisioning interface details.

**Object ID**

2.16.840.1.113894.8.2.16

### **Superior Object Class**

[top](#)

### **Object Class Type**

Auxilliary

### **Required Attributes**

[orclODIPProfileInterfaceType](#), [orclODIPProfileProvSubscriptionMode](#)

### **Allowed Attributes**

[orclODIPProfileStatusUpdate](#), [orclODIPProvInterfaceFilter](#),  
[orclODIPProvInterfaceProcessor](#)

## **7.2.44 orclODIPProvisioningIntegrationInBoundProfileV2**

### **Description**

Configuration for an Oracle Directory Integration and Provisioning profile for imports from third-party directories.

### **Object ID**

2.16.840.1.113894.8.2.402

### **Superior Object Class**

[top](#)

### **Object Class Type**

Structural

### **Required Attributes**

[cn](#), [orclODIPProfileLastAppliedAppEventID](#), [orclODIPProvisioningAppGUID](#),  
[orclODIPProvisioningEventMappingRules](#),  
[orclODIPProvisioningEventPermittedOperations](#)

### **Allowed Attributes**

[orclODIPProfileLastProcessingTime](#), [orclODIPProfileLastSuccessfulProcessingTime](#),  
[orclODIPProfileProcessingErrors](#), [orclODIPProfileProcessingStatus](#), [orclStatus](#)

## **7.2.45 orclODIPProvisioningIntegrationOutBoundProfile**

### **Description**

Configuration for an Oracle Directory Integration and Provisioning profile for exports to third-party directories. This object class is used for profiles created prior to release 10g.

### **Object ID**

2.16.840.1.113894.8.2.404

### **Superior Object Class**

[top](#), [orclChangeSubscriber](#)

**Object Class Type**

Structural

**Required Attributes**

cn, orclODIPProvisioningAppGUID, orclODIPProvisioningEventSubscription

**Allowed Attributes**

orclODIPProfileProvSubscriptionMode, orclODIPProfileLastProcessingTime, orclODIPProfileLastSuccessfulProcessingTime, orclODIPProfileProcessingErrors, orclODIPProfileProcessingStatus, orclStatus, orclVersion

**7.2.46 orclODIPProvisioningIntegrationOutBoundProfileV2****Description**

Configuration for an Oracle Directory Integration and Provisioning profile for exports to third-party directories.

**Object ID**

2.16.840.1.113894.8.2.403

**Superior Object Class**

top, orclChangeSubscriber

**Object Class Type**

Structural

**Required Attributes**

cn, orclODIPProvisioningAppGUID, orclODIPProvisioningEventSubscription

**Allowed Attributes**

orclODIPProfileLastProcessingTime, orclODIPProfileLastSuccessfulProcessingTime, orclODIPProfileProcessingErrors, orclODIPProfileProcessingStatus, orclStatus

**7.2.47 orclODIPProvisioningIntegrationProfile****Description**

Configuration for an Oracle Directory Integration and Provisioning profile for integration with third-party directories. This object class is used for profiles created in releases prior to 10g.

**Object ID**

2.16.840.1.113894.8.2.400

**Superior Object Class**

top, orclODIPIntegrationProfile, orclChangeSubscriber

**Object Class Type**

Structural

**Required Attributes**

orclODIPProvisioningAppName, orclODIPProvisioningAppGUID,  
orclODIPProvisioningOrgName, orclODIPProvisioningOrgGUID,  
orclODIPProvisioningEventSubscription

**Allowed Attributes**

N/A

## 7.2.48 orclODIPProvisioningIntegrationProfileV2

**Description**

Configuration for an Oracle Directory Integration and Provisioning profile for integration with third-party directories.

**Object ID**

2.16.840.1.113894.8.2.401

**Superior Object Class**

top, orclODIPIntegrationProfile

**Object Class Type**

Structural

**Required Attributes**

orclODIPProvisioningAppGUID, orclODIPProvisioningAppName,  
orclODIPProvisioningOrgGUID, orclODIPProvisioningOrgName

**Allowed Attributes**

N/A

## 7.2.49 orclODIPProfile

**Description**

Profile for Oracle Directory Integration and Provisioning server

**Object ID**

2.16.840.1.113894.8.2.1

**Superior Object Class**

top

**Object Class Type**

Structural

**Required Attributes**

N/A

**Allowed Attributes**

orclODIPAgentConfigInfo, orclODIPAgentControl, orclODIPAgentExeCommand, orclODIPAgentHostName, orclODIPAgentName, orclODIPAgentPassword, orclODIPAttributeMappingRules, orclODIPBootStrapStatus, orclODIPConDirAccessAccount, orclODIPConDirAccessPassword, orclODIPConDirLastAppliedChgNum, orclODIPConDirMatchingFilter, orclODIPConDirURL, orclODIPInterfaceType, orclODIPLastExecutionTime, orclODIPLastSuccessfulExecutionTime, orclODIPOIDMatchingFilter, orclODIPProfileDebugLevel, orclODIPSchedulingInterval, orclODIPSynchronizationErrors, orclODIPSynchronizationMode, orclODIPSynchronizationStatus, orclODIPSyncRetryCount, orclVersion, userPassword

**7.2.50 orclODIPSchemaDetails****Description**

Oracle Directory Integration and Provisioning DIT configuration.

**Object ID**

2.16.840.1.113894.8.2.11

**Superior Object Class**

[top](#)

**Object Class Type**

Auxilliary

**Required Attributes**

N/A

**Allowed Attributes**

cn, orclODIPApplicationsLocation, orclODIPInstancesLocation, orclODIPObjectDefnLocation, orclODIPProfileDataLocation, orclODIPProvProfileLocation, orclODIPRootLocation, orclODIPSchemaVersion, orclODIPServerConfigLocation, orclODIPSyncProfileLocation

**7.2.51 orclODIPServerConfig****Description**

Configuration attributes for the Oracle Directory Integration and Provisioning server.

**Object ID**

2.16.840.1.113894.8.2.501

**Superior Object Class**

[top](#)

**Object Class Type**

Auxilliary

**Required Attributes**

N/A

**Allowed Attributes**

cn, orclODIPSearchCountLimit, orclODIPSearchTimeLimit, orclODIPServerCommitSize, orclODIPServerDebugLevel, orclODIPServerRefreshIntvl, orclODIPServerSSLMode, orclODIPServerWalletLoc

## 7.2.52 orclODISConfig

**Description**

Configuration attributes for the Oracle Directory Integration and Provisioning server.

**Object ID**

2.16.840.1.113894.8.2.3

**Superior Object Class**

[top](#)

**Object Class Type**

Structural

**Required Attributes**

cn

**Allowed Attributes**

[orclODIPConfigDNs](#), [orclODIPConfigRefreshFlag](#)

## 7.2.53 orclODIServer

**Description**

Configuration attributes for the Oracle Directory Integration and Provisioning server.

**Object ID**

2.16.840.1.113894.8.2.2

**Superior Object Class**

[top](#)

**Object Class Type**

Structural

**Required Attributes**

N/A

**Allowed Attributes**

cn, orclHostname, orclVersion, userPassword

## 7.2.54 orclODISInstance

**Description**

Configuration attributes for the Oracle Directory Integration and Provisioning server instance.

**Object ID**

2.16.840.1.113894.8.2.4

**Superior Object Class**

[top](#), [orclODISConfig](#)

**Object Class Type**

Structural

**Required Attributes**

[cn](#), [orclconfigsetnumber](#), [orclhostname](#)

**Allowed Attributes**

[description](#), [orclODIPInstanceStatus](#), [orclODIPProfileExecGroupID](#), [orclSSLEnable](#), [seeAlso](#)

## 7.2.55 orclPerfStats

**Description**

Oracle Internet Directory Server Manageability performance statistics.

**Object ID**

2.16.840.1.113894.1.2.26

**Superior Object Class**

N/A

**Object Class Type**

Auxilliary

**Required Attributes**

N/A

**Allowed Attributes**

[orclACLResultsLatency](#), [orclAttrACLEvalLatency](#), [orclBERgenLatency](#), [orclDBLatency](#), [orclDIMEonlyLatency](#), [orclEntryACLEvalLatency](#), [orclFilterACLEvalLatency](#), [orclFrontLatency](#), [orclGenObjLatency](#), [orclGetNearACLLatency](#), [orclOpLatency](#), [orclSQLexeFetchLatency](#), [orclSQLGenReusedParsed](#)

## 7.2.56 orclPKICRL

### Description

Oracle Application Server Certificate Authority certificate revocation list (CRL).

### Object ID

2.16.840.1.113894.2.2.300.1

### Superior Object Class

[crldistributionPoint](#) (RFC 2256)

### Object Class Type

Structural

### Required Attributes

[cn](#)

### Allowed Attributes

[orclPKINextUpdate](#), [x509issuer](#)

## 7.2.57 orclPKIVaIMecCI

### Description

Used by Oracle Application Server Certificate Authority.

### Object ID

2.16.840.1.113894.2.2.300.2

### Superior Object Class

[orclContainer](#)

### Object Class Type

Structural

### Required Attributes

[cn](#)

### Allowed Attributes

[orclPKIVaIMecAttr](#)

## 7.2.58 orclPluginConfig

### Description

Configuration attributes for Oracle Internet Directory plug-ins.

### Object ID

2.16.840.1.113894.1.2.90



**Superior Object Class**[top](#)**Object Class Type**

Structural

**Required Attributes**[cn](#), [orclPluginLDAPOperation](#), [orclPluginName](#), [orclPluginType](#)**Allowed Attributes**[orclPluginAttributeList](#), [orclPluginCheckEntryExist](#), [orclPluginEnable](#), [orclPluginEntryProperties](#), [orclPluginIsReplace](#), [orclPluginKind](#), [orclPluginRequestGroup](#), [orclPluginRequestNegGroup](#), [orclPluginResultCode](#), [orclPluginSASLCallBack](#), [orclPluginSearchNotFound](#), [orclPluginShareLibLocation](#), [orclPluginSubscriberDNList](#), [orclPluginTiming](#), [orclPluginVersion](#)**7.2.59 orclPluginContainer****Description**

Container object for Oracle Internet Directory plug-ins.

**Object ID**

2.16.840.1.113894.1.2.92

**Superior Object Class**[top](#)**Object Class Type**

Structural

**Required Attributes**[cn](#)**Allowed Attributes**[orclPluginPort](#)**7.2.60 orclPluginUser****Description**

Configuration attributes for Oracle Internet Directory plug-ins.

**Object ID**

2.16.840.1.113894.1.2.91

**Superior Object Class**[top](#)**Object Class Type**

Structural

**Required Attributes**

[cn](#), [userPassword](#)

**Allowed Attributes**

[description](#)

## 7.2.61 orclPurgeConfig

**Description**

Configuration attributes for Oracle Internet Directory garbage collectors. Oracle Internet Directory provides several predefined garbage collectors that, together, clean up all unwanted data in the directory server.

**Object ID**

2.16.840.1.113894.1.2.150

**Superior Object Class**

[top](#)

**Object Class Type**

Structural

**Required Attributes**

[cn](#), [orclPurgeBase](#)

**Allowed Attributes**

[orclPurgeDebug](#), [orclPurgeEnable](#), [orclPurgeFileLoc](#), [orclPurgeFileName](#), [orclPurgeFilter](#), [orclPurgeInterval](#), [orclPurgeNow](#), [orclPurgePackage](#), [orclPurgeStart](#), [orclPurgeTargetAge](#), [orclPurgeTranSize](#)

## 7.2.62 orclPwdVerifierPolicy

**Description**

A password verifier policy entry associates a password policy with an application.

**Object ID**

2.16.840.1.113894.1.2.42

**Superior Object Class**

[pwdpolicy](#)

**Object Class Type**

Auxilliary

**Required Attributes**

[orclAppId](#)

**Allowed Attributes**

N/A

## 7.2.63 orclPwdVerifierProfile

### Description

Oracle Internet Directory and other Oracle components both store the user password in the user entry, but use different attributes. A password verifier profile entry associates the correct user password attribute with a component or application.

### Object ID

2.16.840.1.113894.1.2.41

### Superior Object Class

[top](#)

### Object Class Type

Structural

### Required Attributes

[cn](#), [orclAppId](#)

### Allowed Attributes

[displayName](#), [orclPwdVerifierParams](#), [owner](#)

## 7.2.64 orclReplAgreementEntry

### Description

Configuration attributes for replication.

### Object ID

2.16.840.1.113894.1.2.8

### Superior Object Class

[top](#)

### Object Class Type

Structural

### Required Attributes

[orclAgreementId](#), [orclReplicationProtocol](#), [orclUpdateSchedule](#)

### Allowed Attributes

[orclDirReplGroupDSAs](#), [orclExcludedAttributes](#), [orclExcludedNamingContexts](#), [orclHIQSchedule](#), [orclIncludedNamingContexts](#), [orclLastAppliedChangeNumber](#), [orclLDAPConnKeepALive](#), [orclReplicaDN](#)

## 7.2.65 orclReplicaSubentry

### Description

Configuration attributes for replication.

**Object ID**

2.16.840.1.113894.1.2.151

**Superior Object Class**

[top](#)

**Object Class Type**

Structural

**Required Attributes**

[orclReplicaID](#)

**Allowed Attributes**

[orclPilotMode](#), [orclReplicaSecondaryURI](#), [orclReplicaState](#), [orclReplicaType](#), [orclReplicaURI](#), [orclReplicaVersion](#), [pilotStartTime](#), [seeAlso](#)

## 7.2.66 orclReplInstance

**Description**

Configuration attributes for an Oracle Directory Replication server instance.

**Object ID**

2.16.840.1.113894.1.2.14

**Superior Object Class**

[top](#), [orclReplSubConfig](#)

**Object Class Type**

Structural

**Required Attributes**

[cn](#), [orclCompatibleVersion](#), [orclHostname](#)

**Allowed Attributes**

[description](#), [seeAlso](#)

## 7.2.67 orclReplNameCtxConfig

**Description**

Configuration attributes for replication naming contexts.

**Object ID**

2.16.840.1.113894.1.2.104

**Superior Object Class**

[top](#)

**Object Class Type**

Structural

**Required Attributes**

cn, orclIncludedNamingContexts

**Allowed Attributes**

orclExcludedAttributes, orclExcludedNamingContexts

## 7.2.68 orclReplSubConfig

**Description**

Directory Replication server configuration attributes.

**Object ID**

2.16.840.1.113894.1.2.4

**Superior Object Class**

top, orclConfigSet

**Object Class Type**

Structural

**Required Attributes**

cn

**Allowed Attributes**

orclChangeLogLife, orclChangeRetryCount, orclDirReplGroupAgreement, orclPurgeSchedule, orclThreadsPerSupplier

## 7.2.69 orclResourceDescriptor

**Description**

Configuration attributes for a resource.

**Object ID**

2.16.840.1.113894.1.2.65

**Superior Object Class**

top

**Object Class Type**

Structural

**Required Attributes**

orclResourceName

**Allowed Attributes**

description, displayName, orclFlexAttribute1, orclFlexAttribute2, orclFlexAttribute3, orclOwnerGUID, orclPasswordAttribute, orclResourceTypeName, orclResourceViewers, orclUserIDAttribute, orclUserModifiable

## 7.2.70 orclResourceType

### Description

Configuration attributes for resource types.

### Object ID

2.16.840.1.113894.1.2.63

### Superior Object Class

[top](#)

### Object Class Type

Structural

### Required Attributes

[orclResourceTypeName](#)

### Allowed Attributes

[description](#), [javaClassName](#), [orclConnectionFormat](#), [orclFlexAttribute1](#), [orclFlexAttribute2](#), [orclFlexAttribute3](#), [orclPasswordAttribute](#), [orclUserIDAttribute](#)

## 7.2.71 orclRootContext

### Description

Configuration of the Oracle Context.

### Object ID

2.16.840.1.113894.7.2.1006

### Superior Object Class

[top](#)

### Object Class Type

Auxilliary

### Required Attributes

N/A

### Allowed Attributes

[description](#)

## 7.2.72 orclSchemaVersion

### Description

Configuration of the Oracle Context.

### Object ID

2.16.840.1.113894.7.2.6

**Superior Object Class**[top](#)**Object Class Type**

Structural

**Required Attributes**[cn](#), [orclProductVersion](#)**Allowed Attributes**

N/A

**7.2.73 orclSecRefreshEvents****Description**

Oracle Internet Directory Server Manageability attributes for security refresh events.

**Object ID**

2.16.840.1.113894.1.2.28

**Superior Object Class**

N/A

**Object Class Type**

Auxilliary

**Required Attributes**

N/A

**Allowed Attributes**[orclAuditMessage](#), [orclEventType](#), [orclOpResult](#), [orclUserDN](#)**7.2.74 orclService****Description**

Configuration attributes for a service.

**Object ID**

2.16.840.1.113894.7.2.1001

**Superior Object Class**[top](#)**Object Class Type**

Structural

**Required Attributes**[cn](#)

**Allowed Attributes**

[description](#), [orclNetDescName](#), [orclNetDescString](#), [orclOracleHome](#), [orclServiceType](#), [orclSID](#), [orclSystemName](#), [orclVersion](#)

## 7.2.75 orclServiceInstance

**Description**

Configuration attributes for a service instance.

**Object ID**

2.16.840.1.113894.1.2.191

**Superior Object Class**

[top](#)

**Object Class Type**

Structural

**Required Attributes**

[cn](#), [orclServiceType](#)

**Allowed Attributes**

[description](#), [displayName](#), [labeledURI](#), [orclAssocDB](#), [orclAssocInstance](#), [orclEnabled](#), [orclFlexAttribute1](#), [orclMasterNode](#), [orclNetDescName](#), [orclNetDescString](#), [orclOracleHome](#), [orclServiceSubType](#), [orclSID](#), [orclSystemName](#), [orclVersion](#)

## 7.2.76 orclServiceInstanceReference

**Description**

Reference for a service instance.

**Object ID**

2.16.840.1.113894.1.2.200

**Superior Object Class**

N/A

**Object Class Type**

Structural

**Required Attributes**

N/A

**Allowed Attributes**

[cn](#), [description](#), [orclServiceInstanceLocation](#), [orclServiceSubscriptionLocation](#), [seeAlso](#)



## 7.2.77 orclServiceRecipient

**Description**

Additional attributes for a service recipient.

**Object ID**

2.16.840.1.113894.1.2.68

**Superior Object Class**

N/A

**Object Class Type**

Auxilliary

**Required Attributes**

N/A

**Allowed Attributes**

[orclActiveEndDate](#), [orclActiveStartdate](#), [orclIsEnabled](#)

## 7.2.78 orclServiceSubscriptionDetail

**Description**

Service subscription detail.

**Object ID**

2.16.840.1.113894.1.2.201

**Superior Object Class**

orclReferenceObject

**Object Class Type**

Structural

**Required Attributes**

N/A

**Allowed Attributes**

[orclActiveEndDate](#), [orclActiveStartdate](#), [orclIsEnabled](#)

## 7.2.79 orclServiceSuite

**Description**

Configuration for a suite of services.

**Object ID**

2.16.840.1.113894.1.2.193

**Superior Object Class**

[top](#)

**Object Class Type**

Structural

**Required Attributes**

[cn](#), [orclSuiteType](#)

**Allowed Attributes**

[description](#), [displayName](#), [orclEnabled](#), [orclFlexAttribute1](#), [orclServiceMember](#), [orclVersion](#)

## 7.2.80 orclSM

**Description**

Oracle Internet Directory Server Manageability statistics.

**Object ID**

2.16.840.1.113894.1.2.25

**Superior Object Class**

[top](#)

**Object Class Type**

Structural

**Required Attributes**

[orclSequence](#)

**Allowed Attributes**

[orclEventTime](#), [orclHostname](#), [orclLDAPInstanceID](#), [orclLDAPPProcessID](#), [orclSMSpec](#)

## 7.2.81 orclSubscriber

**Description**

Subscriber info for a user entry.

**Object ID**

2.16.840.1.113894.1.2.58

**Superior Object Class**

[top](#)

**Object Class Type**

Auxilliary

**Required Attributes**

N/A

**Allowed Attributes**

c, jpegPhoto, orclContact, orclHostedCreditCardExpireDate, orclHostedCreditCardNumber, orclHostedCreditCardType, orclHostedDunsNumber, orclHostedPaymentTerm, orclSubscriberFullName, orclSubscriberType, orclVersion

**7.2.82 orclSysResourceEvents****Description**

Error log entry for Oracle Internet Directory server.

**Object ID**

2.16.840.1.113894.1.2.29

**Superior Object Class**

N/A

**Object Class Type**

Auxilliary

**Required Attributes**

N/A

**Allowed Attributes**

orclDBConnCreationFailed, orclDNSUnavailable, orclEventType, orclFDIncreaseError, orclMaxFDLimitReached, orclMaxProcessLimitReached, orclMemAllocError, orclNWCongested, orclNwUnavailable, orclORA28error, orclORA3113error, orclORA3114error, orclThreadSpawnFailed

**7.2.83 orclTraceConfig****Description**

Configuration for Oracle Internet Directory Server Manageability.

**Object ID**

2.16.840.1.113894.1.2.31

**Superior Object Class**

[top](#)

**Object Class Type**

Structural

**Required Attributes**

N/A

**Allowed Attributes**

orclTraceDimesionLevel, orclTraceFileLocation, orclTraceFileSize, orclTraceLevel, orclTraceMode

## 7.2.84 orclUniqueConfig

**Description**

Configuration for attributes that must have unique values for each entry that meets the specified requirements.

**Object ID**

2.16.840.1.113894.1.2.103

**Superior Object Class**

[orclCommonAttributes](#)

**Object Class Type**

Structural

**Required Attributes**

[orclUniqueAttrName](#)

**Allowed Attributes**

[orclUniqueEnable](#), [orclUniqueObjectClass](#), [orclUniqueScope](#), [orclUniqueSubtree](#)

## 7.2.85 orclUserStats

**Description**

Oracle Internet Directory Server Manageability statistics for users.

**Object ID**

2.16.840.1.113894.1.2.32

**Superior Object Class**

N/A

**Object Class Type**

Auxilliary

**Required Attributes**

N/A

**Allowed Attributes**

[orclACLResultsLatency](#), [orclAttrACLEvalLatency](#), [orclBERgenLatency](#), [orclDBLatency](#), [orclDIMEonlyLatency](#), [orclEntryACLEvalLatency](#), [orclFilterACLEvalLatency](#), [orclFrontLatency](#), [orclGenObjLatency](#), [orclGetNearACLLatency](#), [orclIpAddress](#), [orclOpAbandoned](#), [orclOpCompleted](#), [orclOpenConn](#), [orclOpFailed](#), [orclOpInitiated](#), [orclOpLatency](#), [orclOpPending](#), [orclOpSucceeded](#), [orclOpTimedOut](#), [orclSQLexeFetchLatency](#), [orclSQLGenReusedParsed](#), [orclUserDN](#)

## 7.2.86 orclUserV2

### Description

Optional attributes for user entries.

### Object ID

2.16.840.1.113894.1.2.52

### Superior Object Class

[top](#)

### Object Class Type

88

### Required Attributes

N/A

### Allowed Attributes

authPassword, c, krbPrincipalName, middleName, orclActiveEndDate, orclActiveStartDate, orclDateOfBirth, orclDefaultProfileGroup, orclDisplayPersonalInfo, orclGender, orclHireDate, orclIsEnabled, orclIsVisible, orclMaidenName, orclPassword, orclPasswordHint, orclPasswordHintAnswer, orclPasswordVerifier, orclPKCS12Hint, orclSAMAccountName, orclSearchFilter, orclTimeZone, orclTxnMaxOperations, orclWirelessAccountNumber, orclWorkflowNotificationPref, userPKCS12

## 7.2.87 pwdpolicy

### Description

Defines password policy information for a set of users in a given DIT. It contains attributes that define the password policy information for the entire directory.

### Object ID

1.3.6.1.4.1.42.2.27.8.2.1

### Superior Object Class

[top](#)

### Object Class Type

Structural

### Required Attributes

cn

### Allowed Attributes

displayName, orclPwdAllowHashCompare, orclPwdAlphaNumeric, orclPwdEncryptionEnable, orclPwdIllegalValues, orclPwdIPLockout, orclPwdIPLockoutDuration, orclPwdIPMaxFailure, orclPwdPolicyEnable, pwdAllowUserChange, pwdCheckSyntax, pwdExpireWarning, pwdFailureCountInterval, pwdGraceLoginLimit, pwdInHistory, pwdLockout,

[pwdLockoutDuration](#), [pwdMaxAge](#), [pwdMaxFailure](#), [pwdMinAge](#), [pwdMinLength](#), [pwdMustChange](#), [pwdSafeModify](#)

## 7.2.88 subentry

### Description

Oracle Internet Directory DIT configuration for subentries.

### Object ID

2.5.17.0

### Superior Object Class

[top](#)

### Object Class Type

Structural

### Required Attributes

[cn](#)

### Allowed Attributes

N/A

## 7.2.89 subregistry

### Description

Oracle Internet Directory DIT configuration.

### Object ID

2.16.840.1.113894.1.2.12

### Superior Object Class

[top](#)

### Object Class Type

Auxilliary

### Required Attributes

[cn](#)

### Allowed Attributes

N/A

## 7.2.90 subschema

### Description

Oracle Internet Directory schema elements.

**Object ID**

2.5.20.1

**Superior Object Class**

N/A

**Object Class Type**

Auxilliary

**Required Attributes**

attributetypes, objectclasses

**Allowed Attributes**

contentRules, ldapSyntaxes, matchingRules

## 7.2.91 tombstone

**Description**

Garbage collector to clean up entries marked as deleted.

**Object ID**

2.16.840.1.113894.1.2.24

**Superior Object Class**[top](#)**Object Class Type**

Structural

**Required Attributes**

N/A

**Allowed Attributes**[ref](#)

## 7.2.92 top

**Description**

Contains common and operational attributes used by various objects in Oracle Internet Directory.

**Object ID**

2.5.6.0

**Superior Object Class**

N/A

**Object Class Type**

Abstract

**Required Attributes**

objectClass

**Allowed Attributes**

authPassword, createTimestamp, creatorsName, modifiersName, modifyTimestamp, orclACI, orclEntryLevelACI, orclGUID, orclNormDN, orclObjectGUID, orclPwAccountUnlock, orclPwIPAAccountLockedTime, orclPwIPFailureTime, orclRevPw, orclUnsyncRevPw, pwdAccountLockedTime, pwdChangedTime, pwdExpirationWarned, pwdFailureTime, pwdGraceUseTime, pwdHistory



---



---

## LDAP Attribute Reference

This chapter provides reference information about the LDAP attributes used for Oracle Identity Management.

This chapter includes the following sections:

- Section 8.1, "Standard LDAP Attributes"
- Section 8.2, "Oracle Identity Management Attribute Reference"

For a list of attributes grouped by functional categories, see Section 6.2, "Overview of Oracle Identity Management Schema Elements."

### 8.1 Standard LDAP Attributes

Oracle Internet Directory supports the following standard LDAP attributes as defined in the Internet Engineering Task Force (IETF) Requests for Comments (RFC) specifications.

Details of RFC specifications can be found on the IETF Web site at: <http://www.ietf.org>.

**Table 8–1 Standard LDAP Attributes Used By Oracle Internet Directory**

Attribute Name	Specification
aliasedObjectName	RFC 2256
applicationEntity	RFC 2256
associatedDomain	RFC 1274
associatedName	RFC 1274
audio	RFC 1274
authorityRevocationList	RFC 2256
authPassword	RFC 3112
bootFile	RFC 2307
bootParameter	RFC 2307
businessCategory	RFC 2256
c	RFC 2256
caCertificate	RFC 2256
carLicense	RFC 2798
certificateRevocationList	RFC 2256

**Table 8–1 (Cont.) Standard LDAP Attributes Used By Oracle Internet Directory**

<b>Attribute Name</b>	<b>Specification</b>
cn	RFC 2256
co	RFC 1274
crossCertificatePair	RFC 2256
dc	RFC 2247
deltaRevocationList	RFC 2256
departmentNumber	RFC 2798
description	RFC 2256
destinationIndicator	RFC 2256
displayName	RFC 2798
dITRedirect	RFC 1274
dmdName	RFC 2256
dNSRecord	RFC 1274
drink	RFC 1274
dSAQuality	RFC 1274
employeeNumber	RFC 2798
employeeType	RFC 2798
facsimileTelephoneNumber	RFC 2256
gecos	RFC 2307
gidNumber	RFC 2307
givenName	RFC 2798
homeDirectory	RFC 2307
homePhone	RFC 1274
homePostalAddress	RFC 1274
host	RFC 1274
initials	RFC 2256
internationalISDNNumber	RFC 2256
ipHostNumber	RFC 2307
ipNetmaskNumber	RFC 2307
ipNetworkNumber	RFC 2307
ipProtocolNumber	RFC 2307
ipServicePort	RFC 2307
ipServiceProtocol	RFC 2307
javaClassName	RFC 2713
javaClassNames	RFC 2307
javaCodebase	RFC 2307
javaDoc	RFC 2307
javaFactory	RFC 2307

**Table 8–1 (Cont.) Standard LDAP Attributes Used By Oracle Internet Directory**

<b>Attribute Name</b>	<b>Specification</b>
javaReferenceAddress	RFC 2713
javaSerializedData	RFC 2713
janetMailbox	RFC 1274
<a href="#">jpegPhoto</a>	RFC 1488
knowledgeInformation	RFC 2256
l	RFC 2256
<a href="#">labeledURI</a>	RFC 2079
lastModifiedBy	RFC 1274
lastModifiedTime	RFC 1274
loginShell	RFC 2307
macAddress	RFC 2307
<a href="#">mail</a>	RFC 2798
mailAlternateAddress	RFC 2256
mailHost	RFC 2256
mailPreferenceOption	RFC 1274
mailRoutingAddress	RFC 2256
manager	RFC 1274
member	RFC 2256
memberNisNetgroup	RFC 2307
memberUid	RFC 2307
mobile	RFC 1274
nisDomain	RFC 2307
nisMapEntry	RFC 2307
nisMapName	RFC 2307
nisNetgroupTriple	RFC 2307
nisPublicKey	RFC 2307
nisSecretKey	RFC 2307
o	RFC 2256
oncRpcNumber	RFC 2307
organizationalStatus	RFC 1274
otherMailbox	RFC 1274
ou	RFC 2256
<a href="#">owner</a>	RFC 2256
pager	RFC 1274
personalSignature	RFC 1274
personalTitle	RFC 1274
photo	RFC 1274

**Table 8–1 (Cont.) Standard LDAP Attributes Used By Oracle Internet Directory**

<b>Attribute Name</b>	<b>Specification</b>
physicalDeliveryOfficeName	RFC 2256
postalAddress	RFC 2256
postalCode	RFC 2256
postOfficeBox	RFC 2256
preferredDeliveryMethod	RFC 2256
preferredDeliveryMethod	RFC 2377
preferredLanguage	RFC 2798
presentationAddress	RFC 2256
protocolInformation	RFC 2256
ref	RFC 3296
registeredAddress	RFC 2256
roleOccupant	RFC 2256
roomNumber	RFC 1274
searchGuide	RFC 2256
secretary	RFC 1274
seeAlso	RFC 2256
serialNumber	RFC 2256
shadowExpire	RFC 2307
shadowFlag	RFC 2307
shadowInactive	RFC 2307
shadowLastChange	RFC 2307
shadowMax	RFC 2307
shadowMin	RFC 2307
shadowWarning	RFC 2307
sn	RFC 2256
st	RFC 2256
street	RFC 2256
subtreeMaximumQuality	RFC 1274
subtreeMinimumQuality	RFC 1274
supportedApplicationContext	RFC 2256
telephoneNumber	RFC 2256
teletexTerminalIdentifier	RFC 2256
telexNumber	RFC 2256
textEncodedORAddress	RFC 2377
title	RFC 2256
uid	RFC 2253
uidNumber	RFC 2307

**Table 8–1 (Cont.) Standard LDAP Attributes Used By Oracle Internet Directory**

Attribute Name	Specification
uniqueIdentifier	RFC 1274
uniqueMember	RFC 2256
userCertificate;binary	RFC 2256
userClass	RFC 1274
userPassword	RFC 2256
userPKCS12	RFC 2798
userSMIMECertificate	RFC 2798
x121Address	RFC 2256
x500UniqueIdentifier	RFC 2256

## 8.2 Oracle Identity Management Attribute Reference

This section contains an alphabetical listing of the Oracle Identity Management attributes. These are the attributes used in entries pertaining to Oracle Internet Directory, Oracle Directory Integration Platform, Oracle Delegated Administration Services, and Oracle Single Sign-On.

---

**Note:** Oracle Fusion Middleware 11g Release 1 (11.1.1) does not include Oracle Single Sign-On or Oracle Delegated Administration Services. Oracle Internet Directory 11g Release 1 (11.1.1), however, is compatible with Oracle Single Sign-On and Oracle Delegated Administration Services 10g (10.1.4.3.0) or later.

---

**See Also:** The chapter on managing system configuration attributes in *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*.

### 8.2.1 attributeMap

#### Description

Attribute mappings used by the POSIX naming directory user agent (DUA).

#### Syntax

1.3.6.1.4.1.1466.115.121.1.26 (IA5 String)

#### Matching Rule

caseIgnoreIA5Match

#### Object ID

1.3.6.1.4.1.11.1.3.1.1.9

## 8.2.2 attributeTypes

**Description**

Attribute types supported by the directory.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.3 (Attribute Type Description)

**Matching Rule**

objectIdentifierFirstComponentMatch

**Object ID**

2.5.21.5

**Other**

Directory operational attribute.

## 8.2.3 authenticationMethod

**Description**

Identifies the type of authentication method used to contact the directory server agent (DSA).

**Syntax**

1.3.6.1.4.1.1466.115.121.1.26 (IA5 String)

**Matching Rule**

caseIgnoreIA5Match

**Object ID**

1.3.6.1.4.1.11.1.3.1.1.6

**Other**

Single-valued attribute.

## 8.2.4 authPassword

**Description**

Attribute for storing a password to an Oracle component when that password is the same as that used to authenticate the user to the directory, namely, `userPassword`. The value in this attribute is synchronized with that in the `userPassword` attribute.

Several different applications can require the user to enter the same clear text password used for the directory, but each application may hash it with a different algorithm. In this case, the same clear text password can become the source of several different password verifiers.

This attribute is multivalued and can contain all the other verifiers that different applications use for this user's clear text password. If the `userpassword` attribute is modified, then the `authpassword` values for all applications are regenerated.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.44{128} (Printable String, 128 character maximum)

**Matching Rule**

octetStringMatch

**Object ID**

1.3.6.1.4.1.4203.1.3.4

## 8.2.5 bindAuthPriv

**Description**

Allows Oracle Internet Directory server to restrict users who can bind to it. The administrator creates an LDAP group entry where only members of the group can bind to the server. Each user entry of users who are allowed to bind to the server must contain an `bindAuthPriv` attribute that points to the group. If a user is not a member of the group, bind requests are rejected. Several other considerations are:

- The `bindAuthPriv` attribute can be a collective attribute that allows specific users to inherit it.
- The LDAP group can be a nested group.
- The administrator must ensure the proper ACL for the `bindAuthPriv` attribute, so that the attribute can be added to a user entry only by an administrator.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.34 (Distinguished Name)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.641

**Other**

Single-valued attribute.

## 8.2.6 bindTimeLimit

**Description**

Maximum time in seconds a POSIX directory user agent (DUA) should allow for a search to complete.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

1.3.6.1.4.1.11.1.3.1.1.4

**Other**

Single-valued attribute.

## 8.2.7 c

**Description**

Specifies the country associated with a user's address.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.5.4.6

**Other**

Single-valued attribute.

## 8.2.8 changeloginfo

**Description**

Attribute that provides additional change log information, such as the value of the client IP address. For example:

```
changeloginfo=clientip>::ffff:10.229.116.104
```

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15

**Matching Rule**

caseIgnoreMatch, caseIgnoreSubstringsMatch

**Object ID**

2.16.840.1.113894.1.1.510

**Other**

Single-valued attribute.

## 8.2.9 changestatus

**Description**

The last change number transported by the replication server.



**Syntax**

DN

**Matching Rule**

DistinguishedNameMatch

**Object ID**

2.16.840.1.113894.1.1.22

**8.2.10 cn****Description**

The common name (nickname) attribute which contains the name of an object. If the object corresponds to a user, it is typically the user's full name. A cn (common name) isn't unique, whereas a dn (distinguished name) is unique.

For example, if ABC corp employs two people with the name John Smith, one in HR and one in Finance then they both would have a cn=John Smith, but they would have unique DNs because the DN would take the form:

```
cn=John Smith, ou=HR, o=ABC or  
cn=John Smith, ou=Finance, o=ABC
```

Where ou= organizational unit, and o=organization

**Syntax**

1.3.6.1.4.1.1466.115.121.1.44 (Printable String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.5.4.3

**8.2.11 contentRules****Description**

Specifies the permissible content of entries of a particular structural object class through the identification of an optional set of auxiliary object classes, mandatory, optional, and precluded attributes.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.16 (DIT Content Rule Description)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.1004

## 8.2.12 createTimestamp

### Description

The time that the entry was created.

### Syntax

1.3.6.1.4.1.1466.115.121.1.24 (Generalized Time)

### Matching Rules

generalizedTimeMatch

### Object ID

2.5.18.1

### Other

Single-valued attribute.

Directory operational attribute.

Not user modifiable.

## 8.2.13 creatorsName

### Description

The DN of the entity (such as a user or an application) that created the entry.

### Syntax

1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

### Matching Rule

distinguishedNameMatch

### Object ID

2.5.18.3

### Other

Single-valued attribute.

Directory operational attribute.

Not user modifiable.

## 8.2.14 credentialLevel

### Description

Identifies the type of credentials a POSIX directory user agent (DUA) should use when binding to the directory server.

### Syntax

1.3.6.1.4.1.1466.115.121.1.26 (IA5 String)

**Matching Rule**

caseIgnoreIA5Match

**Object ID**

1.3.6.1.4.1.11.1.3.1.1.10

**Other**

Single-valued attribute.

**8.2.15 defaultSearchBase****Description**

The default base DN used by a POSIX directory user agent (DUA).

**Syntax**

1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

**Matching Rule**

distinguishedNameMatch

**Object ID**

1.3.6.1.4.1.11.1.3.1.1.1

**Other**

Single-valued attribute.

**8.2.16 defaultSearchScope****Description**

User defined search scope used by a POSIX directory user agent (DUA).

**Syntax**

1.3.6.1.4.1.1466.115.121.1.26 (IA5 String)

**Matching Rule**

N/A

**Object ID**

1.3.6.1.4.1.11.1.3.1.1.12

**Other**

Single-valued attribute.

**8.2.17 defaultServerList****Description**

The IP addresses of the default servers that a directory user agent (DUA) should use in a space separated list. After the servers in [preferredServerList](#) are tried, those default servers on the client's subnet are tried, followed by the remaining default servers, until

a connection is made. At least one server must be specified in either `preferredServerList` or `defaultServerList`. This attribute has no default value.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.26 (IA5 String)

**Matching Rule**

`caseIgnoreIA5Match`

**Object ID**

1.3.6.1.4.1.11.1.3.1.1.0

**Other**

Single-valued attribute.

## 8.2.18 description

**Description**

An optional description for the entry.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15{1024} (Directory String, 1024 character maximum)

**Matching Rule**

`caseIgnoreMatch`

**Object ID**

2.5.4.13

## 8.2.19 displayName

**Description**

The preferred name used when displaying the entry in the GUI tools.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

`caseIgnoreMatch`

**Object ID**

2.16.840.1.113730.3.1.241

**Other**

Single-valued attribute.

## 8.2.20 followReferrals

**Description**

Tells a POSIX directory user agent (DUA) if it should follow referrals returned by a directory server agent (DSA) search result.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.26 (IA5 String)

**Matching Rule**

caseIgnoreIA5Match

**Object ID**

1.3.6.1.4.1.11.1.3.1.1.5

**Other**

Single-valued attribute.

## 8.2.21 javaClassName

**Description**

Fully qualified name of a distinguished Java class or interface.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseExactMatch

**Object ID**

1.3.6.1.4.1.42.2.27.4.1.6

**Other**

Single-valued attribute.

## 8.2.22 jpegPhoto

**Description**

A photograph file in JPEG format.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.28 (Binary)

**Matching Rule**

octetStringMatch

**Object ID**

0.9.2342.19200300.100.1.60

## 8.2.23 krbPrincipalName

### Description

Contains the Kerberos principal name.

### Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

### Matching Rule

caseIgnoreMatch

### Object ID

1.3.18.0.2.4.1091

### Other

Single-valued attribute.

## 8.2.24 labeledURI

### Description

Uniform Resource Locator (URL).

### Syntax

1.3.6.1.4.1.1466.115.121.1.26 (IA5 String)

### Matching Rule

caseExactIA5Match

### Object ID

1.3.6.1.4.1.250.1.57

## 8.2.25 ldapSyntaxes

### Description

Identifies the LDAP syntaxes implemented in the directory schema.

### Syntax

1.3.6.1.4.1.1466.115.121.1.54 (LDAP Syntax Description)

### Matching Rule

objectIdentifierFirstComponentMatch

### Object ID

1.3.6.1.4.1.1466.101.120.16

### Other

Directory operational attribute.

## 8.2.26 mail

### Description

This attribute is defined in RFC 1274. Identifies a user's primary e-mail address (the e-mail address retrieved and displayed by "white-pages" lookup applications).

For example: mail: user.name@example.com

### Syntax

1.3.6.1.4.1.1466.115.121.1.26{256} (IA5 String, 256 character maximum)

### Matching Rule

caseIgnoreIA5Match

### Object ID

0.9.2342.19200300.100.1.3

## 8.2.27 matchingRules

### Description

Identifies the matching rules implemented in the directory schema.

### Syntax

1.3.6.1.4.1.1466.115.121.1.30 (Matching Rule Description)

### Matching Rule

objectIdentifierFirstComponentMatch

### Object ID

2.5.21.4

### Other

Directory operational attribute.

## 8.2.28 middleName

### Description

A user's middle name.

### Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

### Matching Rule

caseIgnoreMatch

### Object ID

1.3.6.1.4.1.1466.101.120.34

## 8.2.29 modifiersName

**Description**

The DN of the entity (such as a user or application) that last updated the entry.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

**Matching Rule**

distinguishedNameMatch

**Object ID**

2.5.18.4

**Other**

Single-valued attribute.

Directory operational attribute.

Not user modifiable.

## 8.2.30 modifyTimestamp

**Description**

The time the entry was last modified.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.24 (Generalized Time)

**Matching Rule**

generalizedTimeMatch

**Object ID**

2.5.18.2

**Other**

Single-valued attribute.

Directory operational attribute.

Not user modifiable.

## 8.2.31 namingContexts

**Description**

Top-level DNs for the naming contexts contained in this server. You must have superuser privileges to publish a DN as a naming context. There is no default value.

This attribute is part of the root DSE (DSA-Specific Entry). The root DSE contains a number of attributes that store information about the directory server itself.



**Syntax**

1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

**Matching Rule**

N/A

**Object ID**

1.3.6.1.4.1.1466.101.120.5

**Other**

DSA operational attribute.

## 8.2.32 objectClass

**Description**

The list of object classes from which this object class is derived.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.38 (Object Identifier)

**Matching Rule**

objectIdentifierMatch

**Object ID**

2.5.4.0

## 8.2.33 objectClasses

**Description**

Defines the object classes which are in force within a subschema.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.37 (Object Class Description)

**Matching Rule**

objectIdentifierFirstComponentMatch

**Object ID**

2.5.21.6

**Other**

Directory operational attribute.

## 8.2.34 objectClassMap

**Description**

A mapping from an object class defined by a directory user agent (DUA) to an object class in an alternative schema used in the directory.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.26 (IA5 String)

**Matching Rule**

N/A

**Object ID**

1.3.6.1.4.1.11.1.3.1.1.11

## 8.2.35 orclACI

**Description**

Access control instructions are stored in the directory as attributes of entries. The orclACI attribute is an operational attribute; it is available for use on every entry in the directory, regardless of whether it is defined for the object class of the entry. It is used by the directory server to evaluate what rights are granted or denied when it receives an LDAP request from a client.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.1 (Access Control Item)

**Matching Rule**

accessDirectiveMatch

**Object ID**

2.16.840.1.113894.1.1.42

## 8.2.36 orclACLResultsLatency

**Description**

Reserved for future use.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.129

**Other**

Single-valued attribute.

## 8.2.37 orclActivateReplication

### Description

Specifies that replication be activated on the replication server designated by `orclOidInstanceName` and `orclOidComponentName`. 1: Start replication server, 0: Stop replication server.

### Syntax

Integer

### Matching Rule

`integerMatch`

### Object ID

2.16.840.1.113894.1.1.616

## 8.2.38 orclActiveConn

### Description

Specifies the number of active connections to the Oracle Internet Directory server, including client LDAP connections and database connections.

### Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

### Matching Rule

`integerMatch`

### Object ID

2.16.840.1.113894.1.1.150

### Other

Single-valued attribute.

## 8.2.39 orclActiveEndDate

### Description

Specifies the date and time beyond which a user account is no longer active and beyond which the user is not allowed to authenticate.

### Syntax

1.3.6.1.4.1.1466.115.121.1.24 (Generalized Time)

### Matching Rule

`generalizedTimeMatch`

### Object ID

2.16.840.1.113894.1.1.339

**Other**

Single-valued attribute.

## 8.2.40 orclActiveStartdate

**Description**

Specifies the date and time that a user account is active and the user is allowed to authenticate. If not specified, then the user is considered active immediately.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.24 (Generalized Time)

**Matching Rule**

generalizedTimeMatch

**Object ID**

2.16.840.1.113894.1.1.330

**Other**

Single-valued attribute.

## 8.2.41 orclActiveThreads

**Description**

Specifies the number of active threads on the Oracle Internet Directory server.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.140

**Other**

Single-valued attribute.

## 8.2.42 orclAgreementId

**Description**

Naming attribute for the replication agreement entry.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.26

**Other**

Single-valued attribute.

**8.2.43 orclagreementtype****Description**

Replication agreement type: '0-OneWay 1-TwoWay, 2-LDAP Multimaster, 3-ASR Multimaster.

**Syntax**

Integer

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.511

**8.2.44 orclAnonymousBindsFlag****Description**

Specifies whether anonymous binds to the directory are allowed or not. If set to 2, anonymous binds are allowed, but only search operations on root DSE entry are allowed for anonymous users. If set to 1, then anonymous binds are allowed. If set to 0 (zero), then anonymous binds are not allowed. The default is 1.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.299

**Other**

Single-valued attribute.

**8.2.45 orclAppFullName****Description**

The full name of an application.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.320

## 8.2.46 orclApplId

**Description**

The unique identifier of an application entry associated with a password verifier.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15{128} (Directory String, 128 characters maximum)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.207

**Other**

Single-valued attribute.

## 8.2.47 orclApplicationAddress

**Description**

The address of the application.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.318

## 8.2.48 orclApplicationCommonName

**Description**

The common name (cn) of the application.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.319

**8.2.49 orclApplicationType****Description**

Identifies the application type, such as Oracle Portal.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.280

**Other**

Single-valued attribute.

**8.2.50 orclAssocDB****Description**

Identifies the associated Oracle Database instance with the application or service.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.1007

**8.2.51 orclAssocInstance****Description**

Identifies the associated Oracle Application Server instance with the application or service.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.1006

## 8.2.52 orclAttrACLEvalLatency

**Description**

Reserved for future use.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.138

**Other**

Single-valued attribute.

## 8.2.53 orclAudCustEvents

**Description**

A comma-separated list of events and category names to be audited. Custom events are only applicable when `orclAudFilterPreset` is Custom.

Examples include:

```
Authentication.SUCCESESONLY,  
Authorization(Permission -eq 'CSFPerfmision')
```

**Syntax**

IA5 String

**Matching Rule**

caseExactIAI5Match

**Object ID**

2.16.840.1.113894.1.1.373

## 8.2.54 orclAudFilterPreset

**Description**

Replaces the audit levels used in 10g (10.1.4.0.1) and earlier releases. Values are None, Low, Medium, All, and Custom.

**Syntax**

IA5 String

**Matching Rule**

caseExactIAI5Match



**Object ID**

2.16.840.1.113894.1.1.372

**8.2.55 orclAuditAttribute****Description**

Identifies the audit attribute.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.58

**8.2.56 orclAuditMessage****Description**

Stores an audit message.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.59

**8.2.57 orclAudSplUsers****Description**

A comma separated list of users for whom auditing is always enabled, even if `orclAudFilterPreset` is `None`.

For example:

```
cn=orcladmin.
```

**Syntax**

IA5 String

**Matching Rule**

caseExactIAI5Match

**Object ID**

2.16.840.1.113894.1.1.374

## 8.2.58 orclBERgenLatency

**Description**

Reserved for future use.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.139

**Other**

Single-valued attribute.

## 8.2.59 orclBlockDNIP

**Description**

An IP address that causes Oracle Internet Directory server to reject any new connections and close any existing connections from that IP address.

---

---

**Note:** You need to use the `subtype` property along with this attribute to configure DN or IP address that needs to be blocked. Use the following subtype:

For DN: `dn`

For IP address: `ip`

Consider the following examples:

```
orclblockdnip;dn: cn=jdoe,ou=abc,c=us
orclblockdnip;ip: ffff:11.234.56.789
```

---

---

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.382

**Other**

Single-valued attribute.

## 8.2.60 orclcachenotifyip

### Description

Configuration attribute that associates a port number with an IP address in order to allow Oracle Internet Directory servers to communicate with each other in a cluster environment when cached data is changed.

The servers communicate with each other using the LDAP protocol. For example, the following LDIF file, which you can load using the `ldapmodify` command, associates port number 5678 with IP address 10.10.10.4 for the `oid1` instance:

```
dn: cn=oid1,cn=osdldapd,cn=subconfigsentry
changetype: modify
add: orclcachenotifyip;5678
orclcachenotifyip;5678: 10.10.10.4
```

When `orclcachenotifyip` is configured for an Oracle Internet Directory instance, the IP address must be local to the node where the instance is running.

### Syntax

1.3.6.1.4.1.1466.115.121.1.44

### Matching Rule

caseIgnoreMatch

### Object ID

2.16.840.1.113894.1.1.640

## 8.2.61 orclCatalogEntryDN

### Description

Contains the DN of the catalog entry.

### Syntax

1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

### Matching Rule

distinguishedNameMatch

### Object ID

2.16.840.1.113894.1.1.50

### Other

Single-valued attribute.

## 8.2.62 orclCategory

### Description

Identifies the business category of a service or an application entity

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.317

## 8.2.63 orclCertExtensionAttribute

**Description**

Holds the `OID` of a field within an extension field of the client certificate.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.38 (Object Identifier)

**Matching Rule**

objectIdentifierMatch

**Object ID**

2.16.840.1.113894.1.1.711

**Other**

Single-valued attribute.

## 8.2.64 orclCertExtensionOID

**Description**

Holds the extension field `OID` of the client certificate.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.38 (Object Identifier)

**Matching Rule**

objectIdentifierMatch

**Object ID**

2.16.840.1.113894.1.1.709

**Other**

Single-valued attribute.

## 8.2.65 orclCertificateHash

**Description**

This is a special catalog attribute used for certificate matching. The value of this attribute is computed by calculating a hash of the user certificate when it is added to Oracle Internet Directory.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.44{128} (Printable String, 128 character maximum)

**Matching Rule**

octetStringMatch

**Object ID**

2.16.840.1.113894.1.1.184

**Other**

Single-valued attribute.

Not user modifiable.

## 8.2.66 orclCertificateMatch

**Description**

This is a special catalog attribute used for certificate matching. The value of this attribute contains the correct matching value to use for a user certificate based on the [orclPKIMatchingRule](#) setting.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.44 (Printable String)

**Matching Rule**

octetStringMatch

**Object ID**

2.16.840.1.113894.1.1.183

**Other**

Single-valued attribute.

Not user modifiable.

## 8.2.67 orclCertMappingAttribute

**Description**

Holds the standard field `OID` of the client certificate.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.708

**Other**

Single-valued attribute.

## 8.2.68 orclChangeLogLife

**Description**

Reserved for future use.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.806

**Other**

Single-valued attribute.

DSA operational attribute.

## 8.2.69 orclChangeRetryCount

**Description**

The number of processing retry attempts for a replication change-entry before being moved to the human intervention queue. The value for this parameter must be equal to or greater than 1 (one).

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.23

**Other**

Single-valued attribute.

DSA operational attribute.

## 8.2.70 orclCommonAutoRegEnabled

**Description**

Specifies if auto-registration is enabled or disabled. Allowed values are 0 (disabled) or 1 (enabled).

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.567

**Other**

Single-valued attribute.

## 8.2.71 orclCommonContextMap

**Description**

Stores the common context map.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.904

**Other**

Single-valued attribute.

## 8.2.72 orclCommonDefaultUserCreateBase

**Description**

Identifies the default user creation base where users are created.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.908

**Other**

Single-valued attribute.

## 8.2.73 orclCommonGroupCreateBase

### Description

Identifies the group creation base under which Oracle Delegated Administration Services creates groups

### Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

### Matching Rule

caseIgnoreMatch

### Object ID

2.16.840.1.113894.1.1.903

## 8.2.74 orclCommonNamingAttribute

### Description

Specifies the name of the attribute that is used as an RDN component when creating a user.

### Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

### Matching Rule

caseIgnoreMatch

### Object ID

2.16.840.1.113894.1.1.900

## 8.2.75 orclCommonNicknameAttribute

### Description

Specifies the name of the attribute that uniquely identifies users.

### Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

### Matching Rule

caseIgnoreMatch

### Object ID

2.16.840.1.113894.7.1.7

### Other

Single-valued attribute.



## 8.2.76 orclCommonSASLRealm

### Description

Identifies the common SASL realm. This attribute contains a string value specifying a subset of related entries under a subscriber realm.

### Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

### Matching Rule

caseIgnoreMatch

### Object ID

2.16.840.1.113894.7.1.20

### Other

Single-valued attribute.

## 8.2.77 orclCommonUserSearchBase

### Description

Identifies the branch that contains user entries.

### Syntax

1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

### Matching Rule

distinguishedNameMatch

### Object ID

2.16.840.1.113894.7.1.10

## 8.2.78 orclCommonVerifierEnable

### Description

If this attribute is enabled then the common verifier is used for all related applications. If this attribute is disabled then each application must setup their own verifier profile.

### Syntax

1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

### Matching Rule

booleanMatch

### Object ID

2.16.840.1.113894.1.1.214

### Other

Single-valued attribute.

## 8.2.79 orclCommonVerifierEnable

### Description

If this attribute is enabled then the common verifier is used for all related applications. If this attribute is disabled then each application must setup their own verifier profile.

### Syntax

1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

### Matching Rule

booleanMatch

### Object ID

2.16.840.1.113894.1.1.214

### Other

Single-valued attribute.

## 8.2.80 orclCompatibleVersion

### Description

The Oracle Internet Directory version. Do not modify this attribute. It must be present for Oracle Internet Directory 11.1.1.6 or later to work with the schema. Values can be:

- orclcompatibleversion 11.1.1.6.0
- orclcompatibleversion 11.1.1.7.0

### Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

### Matching Rule

caseIgnoreMatch

### Object ID

2.16.840.1.113894.1.1.1302

### Other

Multi-valued attribute.

## 8.2.81 orclComputedAttribute

### Description

Attribute that allows a configurable attribute and its value to be dynamically computed based on one or more specific rules.

**See Also:** The "Managing Computed Attributes" chapter in the *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory* for more information.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.44

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.628

**Other**

Multi-valued attribute.

## 8.2.82 orclconflresolution

**Description**

Automatically resolve replication conflicts. When this feature is enabled, conflicts in the Human Intervention Queue are automatically moved to the purge queue if the supplier's schema and consumer's schema match.

**Syntax**

Integer

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.828

## 8.2.83 orclConnectByAttribute

**Description**

The attribute type name that you want to use as the filter for a dynamic group query—for example, manager.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.1001

**Other**

Single-valued attribute.

## 8.2.84 orclConnectBySearchBase

### Description

A naming context in the DIT that you want to use as the base for a dynamic group query—for example, `l=us,dc=mycompany,dc=com`. This attribute is currently not used.

### Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

### Matching Rule

caseIgnoreMatch

### Object ID

2.16.840.1.113894.1.1.1003

### Other

Single-valued attribute.

## 8.2.85 orclConnectByStartingValue

### Description

For a dynamic group query, this specifies the DN of the attribute you specified in the [orclConnectByAttribute](#) attribute—for example, `Anne Smith`.

### Syntax

1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

### Matching Rule

distinguishedNameMatch

### Object ID

2.16.840.1.113894.1.1.1002

### Other

Single-valued attribute.

## 8.2.86 orclConnectionFormat

### Description

Specifies the format used to construct the connect string associated with a resource.

### Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

### Matching Rule

caseIgnoreMatch

### Object ID

2.16.840.1.113894.1.1.354

**Other**

Single-valued attribute.

**8.2.87 orclContact****Description**

Identifies a contact person for an organization or an application.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.332

**Other**

Single-valued attribute.

**8.2.88 orclCryptoScheme****Description**

The hash algorithm used to encrypt passwords that are stored in the directory. Options are: MD4, MD5, No encryption, SHA, SSHA, SHA256, SHA384, SHA512, SSHA256, SSHA384, SSHA512, SMD5, or UNIX Crypt. The default is SSHA.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15{128} (Directory String, 128 characters maximum)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.68

**Other**

Single-valued attribute.

**8.2.89 orclDASAdminModifiable****Description**

Specifies whether administration of this entry is available through Oracle Delegated Administration Services.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

**Matching Rule**

booleanMatch

**Object ID**

2.16.840.1.113894.1.1.324

**Other**

Single-valued attribute.

## 8.2.90 orclDASAttrDispOrder

**Description**

Specifies the display order of an attribute in Oracle Delegated Administration Services.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.341

## 8.2.91 orclDASAttrName

**Description**

Specifies the name of an attribute to show in Oracle Delegated Administration Services.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.340

## 8.2.92 orclDASEnableProductLogo

**Description**

Specifies whether to display a product logo on the Identity Management Realm Configuration window of Oracle Delegated Administration Services. Allowed values are TRUE or FALSE.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

**Matching Rule**

booleanMatch

**Object ID**

2.16.840.1.113894.1.1.362

**Other**

Single-valued attribute.

**8.2.93 orclDASEnableSubscriberLogo****Description**

Specifies whether to display a realm logo on the Identity Management Realm Configuration window of Oracle Delegated Administration Services. Allowed values are TRUE or FALSE.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

**Matching Rule**

booleanMatch

**Object ID**

2.16.840.1.113894.1.1.361

**Other**

Single-valued attribute.

**8.2.94 orclDASIsEnabled****Description**

Specifies whether an attribute is enabled for Oracle Delegated Administration Services. Allowed values are TRUE or FALSE.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

**Matching Rule**

booleanMatch

**Object ID**

2.16.840.1.113894.1.1.344

**Other**

Single-valued attribute.

## 8.2.95 orclDASIsMandatory

**Description**

Specifies whether an attribute is mandatory for Oracle Delegated Administration Services. Allowed values are TRUE or FALSE.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

**Matching Rule**

booleanMatch

**Object ID**

2.16.840.1.113894.1.1.321

**Other**

Single-valued attribute.

## 8.2.96 orclDASIsPersonal

**Description**

Specifies whether an attribute is personal information to be supplied by a user in Oracle Delegated Administration Services. Allowed values are TRUE or FALSE.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

**Matching Rule**

booleanMatch

**Object ID**

2.16.840.1.113894.1.1.326

**Other**

Single-valued attribute.

## 8.2.97 orclDASLOV

**Description**

The list of values to display to users in the UI when the `orclDASUIType=Predefined List`.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreSubStringsMatch



**Object ID**

2.16.840.1.113894.1.1.328

**8.2.98 orclDASPublicGroupDNs****Description**

Specifies the DN's of groups available for Oracle Delegated Administration Services.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

**Matching Rule**

distinguishedNameMatch

**Object ID**

2.16.840.1.113894.1.1.343

**8.2.99 orclDASSearchable****Description**

Specifies whether or not this attribute is searchable in Oracle Delegated Administration Services. Allowed values are TRUE or FALSE.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

**Matching Rule**

booleanMatch

**Object ID**

2.16.840.1.113894.1.1.906

**Other**

Single-valued attribute.

**8.2.100 orclDASSearchCollIndex****Description**

Indicates the position in the DAS search result table column, if present.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.902

**Other**

Single-valued attribute.

### 8.2.101 orclDASSearchFilter

**Description**

Specifies whether the attribute is searchable through Oracle Delegated Administration Services. Allowed values are TRUE or FALSE.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

**Matching Rule**

booleanMatch

**Object ID**

2.16.840.1.113894.1.1.325

**Other**

Single-valued attribute.

### 8.2.102 orclDASSearchSizeLimit

**Description**

The maximum number of entries to return in a Oracle Delegated Administration Services search.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.363

**Other**

Single-valued attribute.

### 8.2.103 orclDASSelfModifiable

**Description**

Specifies whether an attribute is modifiable by the user in Oracle Delegated Administration Services. Allowed values are TRUE or FALSE.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

**Matching Rule**

booleanMatch

**Object ID**

2.16.840.1.113894.1.1.322

**Other**

Single-valued attribute.

**8.2.104 orcIDASUIType****Description**

Specifies the UI field type for an attribute when displayed in Oracle Delegated Administration Services. Options are:

- Single Line Text
- Multi Line Text
- Predefined List
- Date
- Browse and Select
- Number

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreSubStringsMatch

**Object ID**

2.16.840.1.113894.1.1.327

**Other**

Single-valued attribute.

**8.2.105 orcIDASURL****Description**

The corresponding URL of an Oracle Delegated Administration Services unit.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.310

## 8.2.106 orclDASURLBase

### Description

This holds the URL base in install area for Oracle Delegated Administration Services.

### Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

### Matching Rule

caseIgnoreMatch

### Object ID

2.16.840.1.113894.1.1.345

## 8.2.107 orclDASValidatePwdReset

### Description

Specifies whether this attribute can be used for password reset validation purposes in Oracle Delegated Administration Services. Allowed values are TRUE or FALSE.

### Syntax

1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

### Matching Rule

booleanMatch

### Object ID

2.16.840.1.113894.1.1.905

### Other

Single-valued attribute.

## 8.2.108 orclDASViewable

### Description

Specifies whether this attribute is viewable through Oracle Delegated Administration Services. Allowed values are TRUE or FALSE.

### Syntax

1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

### Matching Rule

booleanMatch

### Object ID

2.16.840.1.113894.1.1.323

### Other

Single-valued attribute.

## 8.2.109 orclDataprivacymode

**Description**

Data Privacy mode. Sensitive attributes encrypted when returned.

0: Disabled, 1: Enabled

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.890

## 8.2.110 orclDateOfBirth

**Description**

Specifies the date on which a user was born.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.24 (Generalized Time)

**Matching Rule**

generalizedTimeMatch

**Object ID**

2.16.840.1.113894.1.1.307

**Other**

Single-valued attribute.

## 8.2.111 orclDBConnCreationFailed

**Description**

Indicates a connection failure to the database in an error log entry.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.155

**Other**

Single-valued attribute.

## 8.2.112 orclDBLatency

**Description**

Reserved for future use.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.130

**Other**

Single-valued attribute.

## 8.2.113 orclDBSchemaIdentifier

**Description**

DN of the DB registration entry in OID that an application entity uses.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

**Matching Rule**

distinguishedNameMatch

**Object ID**

2.16.840.1.113894.1.1.347

## 8.2.114 orclDBType

**Description**

The type of database used. This attribute is part of the root DSE (DSA-Specific Entry). The root DSE contains a number of attributes that store information about the directory server itself.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15{128} (Directory String, 128 character maximum)

**Matching Rule**

caseIgnoreMatch, caseIgnoreSubstringsMatch

**Object ID**

2.16.840.1.113894.1.1.5

**Other**

Single-valued attribute.

## 8.2.115 orclDebugFlag

### Description

The debug level associated with a server instance. The default is 0 (zero). The valid range is 0 to 402653184.

### Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

### Matching Rule

caseIgnoreMatch

### Object ID

2.16.840.1.113894.1.1.97

### Other

Single-valued attribute.

## 8.2.116 orclDebugForceFlush

### Description

Specifies whether debug messages are to be written to the log file when a message is logged by the directory server. To enable it, set its value to 1. To disable it set it to 0, which is its default value.

### Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

### Matching Rule

integerMatch

### Object ID

2.16.840.1.113894.1.1.193

### Other

Single-valued attribute.

## 8.2.117 orcldebuglevel

### Description

Replication server debug level.

Values are additive:

0: No Debug Log, 2097152: Replication Performance Log, 4194304: Replication Debug Log, 8388608: Function Call Trace, 16777216: Heavy Trace Log

### Syntax

Integer

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.3

**8.2.118 orclDebugOp****Description**

To make logging more focused, limits logged information to particular directory server operations by specifying the debug dimension to those operations. Values for operations are:

- 1 - ldapbind
- 2 - ldapunbind
- 4 - ldapadd
- 8 - ldapdelete
- 16 - ldapmodify
- 32 - ldapmodrdn
- 64 - ldapcompare
- 128 - ldapsearch
- 264 - ldapabandon
- 511 - all operations

To log more than one operation, add the values of their dimensions. For example, if you want to trace ldapbind (1), ldapadd (4) and ldapmodify (16) operations, then the value would be 21 (1 + 4 + 16 = 21).

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.601

**Other**

Single-valued attribute.

**8.2.119 orclDefaultProfileGroup****Description**

Holds the DN of the group to designate the default group for a user, such that a default profile can be built for the user based on this attribute value.



**Syntax**

1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

**Matching Rule**

distinguishedNameMatch

**Object ID**

2.16.840.1.113894.1.1.309

**Other**

Single-valued attribute.

**8.2.120 orclDefaultSubscriber****Description**

Identifies the default realm.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

**Matching Rule**

distinguishedNameMatch

**Object ID**

2.16.840.1.113894.1.1.312

**8.2.121 orclDIMEonlyLatency****Description**

Reserved for future use.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.131

**Other**

Single-valued attribute.

**8.2.122 orclDIPRepository****Description**

Used to determine if the directory is used as the Oracle Directory Integration and Provisioning repository.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.124

**Other**

Single-valued attribute.

## 8.2.123 orclDirectoryVersion

**Description**

The version of Oracle Internet Directory. This attribute is part of the root DSE (DSA-Specific Entry). The root DSE contains a number of attributes that store information about the directory server itself.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.67

**Other**

Single-valued attribute.

## 8.2.124 orclDirReplGroupAgreement

**Description**

Contains the directory replication group agreement DN.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

**Matching Rule**

N/A

**Object ID**

2.16.840.1.113894.1.1.25

**Other**

DSA operational attribute.

## 8.2.125 orclDirReplGroupDSAs

**Description**

For Oracle Database Advanced Replication-based directory replication groups (DRGs), the `orclReplicaID` values of all the nodes in the DRG. This list must be identical on all nodes in the group. This attribute is not applicable for LDAP-based replication agreements.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

N/A

**Object ID**

2.16.840.1.113894.1.1.48

**Other**

DSA operational attribute.

## 8.2.126 orclDisplayPersonalInfo

**Description**

Specifies if the user's personal information should be displayed in white pages queries. Allowed values are TRUE or FALSE.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

**Matching Rule**

booleanMatch

**Object ID**

2.16.840.1.113894.1.1.304

**Other**

Single-valued attribute.

## 8.2.127 OrclDispThreads

**Description**

Number of dispatcher threads per server process.

**Syntax**

Integer

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.613

**8.2.128 orclDITRoot****Description**

The root of the directory information tree (DIT). This attribute is part of the root DSE (DSA-Specific Entry). The root DSE contains a number of attributes that store information about the directory server itself.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15{128} (Directory String, 128 character maximum)

**Matching Rule**

caseIgnoreMatch, caseIgnoreSubStringsMatch

**Object ID**

2.16.840.1.113894.1.1.7

**Other**

Single-valued attribute.

**8.2.129 orclDNSUnavailable****Description**

Reserved for future use.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.161

**Other**

Single-valued attribute.

**8.2.130 orclcachemaxsize****Description**

Specifies the size in bytes of the result set cache or the metadata cache, depending on the subtype:

- rs: Result set cache. Default and minimum cache size is 64 MB.
- md: Metadata cache. Default and minimum cache size is 128 MB.

Specify the size as M or G, indicating megabytes or gigabytes, respectively. To set a subtype, specify:

```
orclcachemaxsize; subtypename: value
```

For example:

```
orclcachemaxsize; md: 256M
```

**Syntax**

1.3.6.1.4.1.1466.115.121.1.44 (Printable String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.642

**Other**

Single-valued attribute.

## 8.2.131 orclEcacheEnabled

**Description**

Specifies whether to enable or disable the Entry Cache or Result Set Cache. Values can be:

- 0: Disable both the Entry Cache and Result Set Cache.
- 1: Enable the Entry Cache only (default value).
- 2: Enable both the Entry Cache and Result Set Cache.

If you change the attribute value, restart the Oracle Internet Directory server instance for the new value to take effect.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.400

**Other**

Single-valued attribute.

## 8.2.132 orclEcacheHitRatio

**Description**

Stores the cache hit ratio.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.170

**Other**

Single-valued attribute.

## 8.2.133 orclEcacheMaxEntries

**Description**

Maximum number of entries that can be present in the entry cache. The default is 25,000.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.402

**Other**

Single-valued attribute.

## 8.2.134 orclEcacheMaxSize

**Description**

Size of shared memory that can be used for the entry cache. The default is 100 MB. Specify the size as M or G, indicating megabytes or gigabytes, respectively.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.401

**Other**

Single-valued attribute.

## 8.2.135 orclEcacheNumEntries

**Description**

The number of entries currently in the entry cache.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.171

**Other**

Single-valued attribute.

## 8.2.136 orclEcacheSize

**Description**

The current size of the entry cache.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.172

**Other**

Single-valued attribute.

## 8.2.137 orclEnabled

**Description**

Determines whether an application is enabled or disabled for use.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

**Matching Rule**

booleanMatch

**Object ID**

2.16.840.1.113894.1.1.1008

**Other**

Single-valued attribute.

**8.2.138 orclEnableGroupCache****Description**

Whether to cache privilege groups and ACL groups. Using this cache improves the performance of access control evaluation for users.

Use the group cache when a privilege group membership does not change frequently. If a privilege group membership does change frequently, then it is best to turn off the group cache. This is because, in such a case, computing a group cache increases overhead. The default is 1 (enabled). Change to 0 (zero) to disable.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.403

**Other**

Single-valued attribute.

**8.2.139 orclencryptedattributes****Description**

List of attributes to be stored in an encrypted form.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.419

**8.2.140 orclEntryACLEvalLatency****Description**

Reserved for future use.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)



**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.136

**Other**

Single-valued attribute.

**8.2.141 orclEntryLevelACI****Description**

Specifies the ACI that holds object level ACL.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.1 (Access Control Item)

**Matching Rule**

accessDirectiveMatch

**Object ID**

2.16.840.1.113894.1.1.43

**8.2.142 orclEventLevel****Description**Specifies critical events related to security and system resources to be recorded for server manageability statistics. The default value is 0. [Table 8-2](#) lists the level values.**Table 8-2 Event Levels**

Level Value	Critical Event	Information It Provides
1	Superuser login	Super uses bind (successes or failures)
2	Proxy user login	Proxy user bind (failures)
4	Replication login	Replication bind (failures)
8	Add access	Add access violation
16	Delete access	Delete access violation
32	Write access	Write access violation
64	ORA 3113 error	Loss of connection to database
128	ORA 3114 error	Loss of connection to database
256	ORA 28 error	ORA-28 Error
512	ORA error	ORA errors other an expected 1, 100, or 1403
1024	Oracle Internet Directory server termination count	
2047	All critical events	

For events other than superuser, proxy user, and replication login, set the value of the `orclStatsFlag` attribute to 1.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.195

**Other**

Single-valued attribute.

### 8.2.143 orclEventTime

**Description**

The time that a logged directory event occurred.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.60

### 8.2.144 orclEventType

**Description**

The type of logged directory event.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.57

### 8.2.145 orclExcludedAttributes

**Description**

Specifies an attribute (within the specified naming context) to be excluded from replication. Applies to partial replication only.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

N/A

**Object ID**

2.16.840.1.113894.1.1.506

**Other**

DSA operational attribute.

## 8.2.146 orclExcludedNamingContexts

**Description**

For Oracle Database Advanced Replication-based agreements, this attribute specifies one or more subtrees to be excluded from replication.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

**Matching Rule**

N/A

**Object ID**

2.16.840.1.113894.1.1.47

**Other**

DSA operational attribute.

## 8.2.147 orclFDIncreaseError

**Description**

Reserved for future use.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.163

**Other**

Single-valued attribute.

## 8.2.148 orclFilterACLEvalLatency

### Description

Reserved for future use.

### Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

### Matching Rule

integerMatch

### Object ID

2.16.840.1.113894.1.1.137

### Other

Single-valued attribute.

## 8.2.149 orclFlexAttribute1

### Description

An additional attribute for storing more information about a resource, service, or component.

### Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

### Matching Rule

caseIgnoreMatch, caseIgnoreSubStringsMatch

### Object ID

2.16.840.1.113894.1.1.355

## 8.2.150 orclFlexAttribute2

### Description

An additional attribute for storing more information about a resource, service, or component.

### Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

### Matching Rule

caseIgnoreMatch, caseIgnoreSubStringsMatch

### Object ID

2.16.840.1.113894.1.1.356

## 8.2.151 orclFlexAttribute3

**Description**

An additional attribute for storing more information about a resource, service, or component.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch, caseIgnoreSubStringsMatch

**Object ID**

2.16.840.1.113894.1.1.357

## 8.2.152 orclFrontLatency

**Description**

Reserved for future use.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.128

**Other**

Single-valued attribute.

## 8.2.153 orclGender

**Description**

The gender of a user.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.346

**Other**

Single-valued attribute.

## 8.2.154 orclgeneratechangelog

### Description

Enables change log generation 1-generate change log, 0-Do not generate change log

### Syntax

Integer

### Matching Rule

integerMatch

### Object ID

2.16.840.1.113894.1.1.617

## 8.2.155 orclGenObjLatency

### Description

Stores the general object latency.

### Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

### Matching Rule

integerMatch

### Object ID

2.16.840.1.113894.1.1.133

### Other

Single-valued attribute.

## 8.2.156 orclGetNearACLLatency

### Description

Reserved for future use.

### Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

### Matching Rule

integerMatch

### Object ID

2.16.840.1.113894.1.1.135

### Other

Single-valued attribute.

## 8.2.157 orclGlobalID

**Description**

Specifies the attribute that is used to identify the global ID of a user.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.7.1.8

**Other**

Single-valued attribute.

## 8.2.158 orclGUID

**Description**

This is the global unique identifier for an entry within Oracle Internet Directory. The value for this attribute is automatically generated when an entry is created and remains constant, even if an entry is moved.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch, caseIgnoreSubStringsMatch

**Object ID**

2.16.840.1.113894.1.1.37

**Other**

Single-valued attribute.

Directory operational attribute.

Not user modifiable.

## 8.2.159 orclGUPassword

**Description**

Password for the guest user account in Oracle Internet Directory.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15{128} (Directory String, 128 character maximum)

**Matching Rule**

caseIgnoreMatch, caseIgnoreSubStringsMatch

**Object ID**

2.16.840.1.113894.1.1.12

**Other**

Single-valued attribute.

**8.2.160 orclHashedAttributes****Description**

List of attributes whose values are hashed, using the crypto scheme set in the root DSE attribute `orclcryptoscheme`.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (caseIgnoreSubstringsMatch)

**Matching Rule**

caseIgnoreSubstringsMatch

**Object ID**

2.16.840.1.113894.1.1.376

**Other**

Multi-valued attribute

---

---

**Notes:**

- Never include the same attribute in both `orclhashedattributes` and `orclencryptedattributes`.
  - Only single-valued attributes can be hashed attributes.
- 
- 

**8.2.161 orclHIQSchedule****Description**

The interval, in seconds, at which the directory replication server repeats the change application process.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

N/A

**Object ID**

2.16.840.1.113894.1.1.98

**Other**

Single-valued attribute.

DSA operational attribute.



## 8.2.162 orclHireDate

**Description**

Specifies the date on which a user was hired by the organization.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.24 (Generalized Time)

**Matching Rule**

generalizedTimeMatch

**Object ID**

2.16.840.1.113894.1.1.308

**Other**

Single-valued attribute.

## 8.2.163 orclHostedCreditCardExpireDate

**Description**

The credit card expiration date for a subscriber.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.338

**Other**

Single-valued attribute.

## 8.2.164 orclHostedCreditCardNumber

**Description**

The credit card number for a subscriber.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.337

**Other**

Single-valued attribute.

## 8.2.165 orclHostedCreditCardType

**Description**

The credit card type for a subscriber.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.336

**Other**

Single-valued attribute.

## 8.2.166 orclHostedDunsNumber

**Description**

The DUNS number of a business subscriber. DUNS (Data Universal Numbering System) is a unique nine character company identification number issued by Dun and Bradstreet Corporation used to identify a US corporate entity.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.334

**Other**

Single-valued attribute.

## 8.2.167 orclHostedPaymentTerm

**Description**

Payment terms for a subscriber account.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.335

**Other**

Single-valued attribute.

**8.2.168 orclHostname****Description**

The host name of the Oracle Internet Directory server.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15{128} (Directory String, 128 character maximum)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.41

**Other**

Single-valued attribute.

**8.2.169 orclIdleConn****Description**

The number of open connections that are currently inactive. Oracle Internet Directory tracks the idle connections for server manageability statistics.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.151

**Other**

Single-valued attribute.

**8.2.170 orclIdleThreads****Description**

The number of Oracle Internet Directory server process threads that are currently inactive. Oracle Internet Directory tracks the idle threads for server manageability statistics.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.141

**Other**

Single-valued attribute.

**8.2.171 orclIncludedNamingContexts****Description**

The naming context included in a partial replica. For each naming context object, you can specify only one unique subtree.

In partial replication, except for subtrees listed in the [orclExcludedNamingContexts](#) attribute, all subtrees in the specified included naming context are replicated.

Only LDAP-based replication agreements respect this attribute to define one or more partial replicas. If this attribute contains any values in an Oracle Database Advanced Replication-based replication agreement, then it is ignored.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

**Matching Rule**

N/A

**Object ID**

2.16.840.1.113894.1.1.819

**Other**

Single-valued attribute.

DSA operational attribute.

**8.2.172 orclIndexedAttribute****Description**

Attributes that are indexed in the Oracle Internet Directory catalog.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.49

**8.2.173 orclInitialServerMemSize****Description**

The memory size of the Oracle Internet Directory server at start up.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.147

**Other**

Single-valued attribute.

**8.2.174 orclinmemfiltprocess****Description**

Search filters to be processed in memory.

**Syntax**

Printable String

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.608

**Other**

Multiple-valued attribute.

**8.2.175 orclInterval****Description**

Time interval in seconds between executions of Oracle Directory Integration and Provisioning profiles.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch, caseIgnoreSubStringsMatch

**Object ID**

2.16.840.1.113894.9.1.8

## 8.2.176 orclIpAddress

**Description**

The IP address of the Oracle Internet Directory server host.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.186

## 8.2.177 orclIsEnabled

**Description**

Whether a user or service subscriber is enabled in Oracle Internet Directory.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.316

**Other**

Single-valued attribute.

## 8.2.178 orclIsVisible

**Description**

This attribute is used to determine if users or groups is visible to applications managed by Oracle Delegated Administration Services, such as Oracle Portal. Oracle Single Sign-On does not use this attribute. Allowed values are TRUE or FALSE.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

**Matching Rule**

booleanMatch

**Object ID**

2.16.840.1.113894.1.1.303

**Other**

Single-valued attribute.

**8.2.179 orclLastAppliedChangeNumber****Description**

For Oracle Directory Integration and Provisioning export operations, the last change from Oracle Internet Directory that was applied to the connected directory. The default value is 0. If you have used the Oracle Directory Integration and Provisioning Assistant to bootstrap the connected directory, then this value is set automatically at the end of the bootstrapping process. This is valid only in the export profile.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.69

**Other**

Single-valued attribute.

**8.2.180 orclLastLoginTime****Description**

Last login time of a user

**Syntax**

1.3.6.1.4.1.1466.115.121.1.24

**Matching Rule**

generalizedTimeMatch

**Object ID**

2.16.840.1.113894.1.1.378

**Other**

Single-valued attribute

**8.2.181 orclLDAPConnKeepALive****Description**

For replication, whether to keep the LDAP connection to the connected directory alive due to activity. If not set Oracle Internet Directory will drop inactive connections after a period of time. Allowed values are TRUE or FALSE.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

**Matching Rule**

booleanMatch

**Object ID**

2.16.840.1.113894.1.1.822

**Other**

Single-valued attribute.

## 8.2.182 orclLDAPConnTimeout

**Description**

The number of minutes before Oracle Internet Directory times out and drops an inactive connection.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.194

**Other**

Single-valued attribute.

## 8.2.183 orclLDAPInstanceID

**Description**

The instance number of a particular Oracle Internet Directory server instance.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.125

**Other**

Single-valued attribute.



## 8.2.184 orclLDAPProcessID

**Description**

The process ID of a particular Oracle Internet Directory server instance.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.126

**Other**

Single-valued attribute.

## 8.2.185 orclMaidenName

**Description**

The maiden name of a user.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.306

## 8.2.186 orclMappedDN

**Description**

Holds the required information for generating the mapped identity.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

**Matching Rule**

distinguishedNameMatch

**Object ID**

2.16.840.1.113894.1.1.704

**Other**

Single-valued attribute.

## 8.2.187 orclMaskFilter

**Description**

LDAP filter specifying entries to be exposed. Others are masked.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.44 (Printable String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.427

**Other**

Multivalued, User-modifiable

## 8.2.188 orclMaskRealm

**Description**

List of DIT subtrees that are exposed or hidden:

- orclMaskRealm contains the DIT subtrees that are exposed in an instance. This attribute is configured in the instance level. The DN configured and its children are visible in the instance. Other entries in the DIT are masked (hidden) for all LDAP operations.
- orclMaskRealm;disallowed contains the DIT subtrees that are hidden in a container for an entire directory for all LDAP operations. This attribute is configured in the DSA configuration entry.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.34 (DN)

**Matching Rule**

distinguishedNameMatch

**Object ID**

2.16.840.1.113894.1.1.426

**Other**

Multivalued, User-modifiable.

## 8.2.189 orclMasterNode

**Description**

Reserved for future use.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

**Matching Rule**

booleanMatch

**Object ID**

2.16.840.1.113894.1.1.1010

**Other**

Single-valued attribute.

**8.2.190 orclMatchDnEnabled****Description**

If the base DN of a search request is not found, then the directory server returns the nearest DN that matches the specified base DN. Whether the directory server tries to find the nearest match DN is controlled by this attribute. If set to 1, then match DN processing is enabled. If set to 0, then match DN processing is disabled. The default is 1.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.404

**Other**

Single-valued attribute.

**8.2.191 orclMaxCC****Description**

The number of connections established by the Oracle Internet Directory server to its backend data base. The default value is 2.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.4

**Other**

Single-valued attribute.

## 8.2.192 orclMaxConnInCache

### Description

The number of connection DNs whose privileged groups can be cached is controlled by orclMaxConnInCache in the instance-specific configuration entry. The default value is 100000 identities (connection DNs). Increase the value of orclMaxConnInCache if your installation has more than 25000 users.

**See Also:** *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory* for more information.

### Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

### Matching Rule

integerMatch

### Object ID

2.16.840.1.113894.1.1.605

### Other

Single-valued attribute.

## 8.2.193 orclmaxLatencyLog

### Description

Time in micro seconds after which any Oracle Internet Directory server operations that exceed this time are logged to the alert log. Default is 500 micro seconds, and the minimum value is 10 micro seconds.

### Syntax

1.3.6.1.4.1.1466.115.121.1.44 (Printable String)

### Matching Rule

caseIgnoreMatch

### Object ID

2.16.840.1.113894.1.1.643

### Other

Single-valued attribute.

## 8.2.194 orclMaxTcpldleConnTime

### Description

Frequency in minutes at which the Oracle Internet Directory server calls OCIPing() to send keep alive messages to the Oracle Database. Setting this attribute to a value less than the timeout value of the firewall between Oracle Internet Directory server and its Database (typically 30 minutes) prevents the Database connection from being dropped.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.196

**Other**

Single-valued attribute.

**8.2.195 orclMaxFDLimitReached****Description**

Reserved for future use.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.156

**Other**

Single-valued attribute.

**8.2.196 orclmaxfiltsize****Description**

Max size of the filter to be allowed for ldap search operation.

**Syntax****Matching Rule****Object ID**

2.16.840.1.113894.1.1.610

**8.2.197 OrclMaxLdapConns****Description**

Max LDAP connections per server.

**Syntax**

Integer

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.611

## 8.2.198 orclmaxlogfiles

**Description**

Maximum number of log files to keep in rotation.

**Syntax**

Integer

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.615

## 8.2.199 orclmaxlogfilesize

**Description**

Maximum size of the log file.

**Syntax**

Integer

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.614

## 8.2.200 orclmaxpsearchconns

**Description**

Maximum number of connections allowed for LDAP persistent search operations. Because persistent search operations keep connections from an LDAP client to the Oracle Internet Server server alive, this attribute can prevent the LDAP connection limit from being reached. Default is 0 (disabled).

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.383

**Other**

Single-valued attribute.

**8.2.201 orclMaxProcessLimitReached****Description**

Reserved for future use.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.164

**Other**

Single-valued attribute.

**8.2.202 orclMaxServerRespTime****Description**

Maximum Time in seconds for Server process to respond back to Dispatcher process

**Syntax**

Integer

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.620

**8.2.203 orclMemAllocError****Description**

Reserved for future use.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.162

**Other**

Single-valued attribute.

**8.2.204 orclMemberOf****Description**

This attribute contains the groups to which the entry belongs. This includes static groups and dynamic groups of objectclass orclDynamicGroup, using labeleduri attribute, which are cached. The membership includes both direct groups and nested groups. The attribute values are computed during search and are not stored. As of Oracle Internet Directory 11g Release 1 (11.1.1.7.0), this attribute can be used in search filters.

orclMemberOf is an operational attribute and is returned by a search only when explicitly requested in the required attributes list.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

**Matching Rule**

distinguishedNameMatch

**Object ID**

2.16.840.1.113894.1.1.424

**Other**

Directory operational attribute.

Not user modifiable.

Aliases: memberof, ismemberof.

**8.2.205 orclNetDescName****Description**

The DN of an Oracle Net Service description entry. Oracle Net directory naming allows net service names to be stored in and retrieved from Oracle Internet Directory.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

**Matching Rule**

distinguishedNameMatch



**Object ID**

2.16.840.1.113894.3.1.12

**Other**

Single-valued attribute.

**8.2.206 orclNetDescString****Description**

The description string for an Oracle Net Service. For example:

```
(DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP) (HOST =  
hostname)(PORT =1521))) (CONNECT_DATA = (SID = ORCL)))
```

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.3.1.13

**Other**

Single-valued attribute.

**8.2.207 orclNonSSLPort****Description**

The non-SSL LDAP listening port for Oracle Internet Directory server.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.102

**Other**

Single-valued attribute.

**8.2.208 orclNormDN****Description**

Identifies the normalized DN of an entry.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

**Matching Rule**

distinguishedNameMatch

**Object ID**

2.16.840.1.113894.1.1.1000

**Other**

Single-valued attribute.

Directory operational attribute.

Not user modifiable.

## 8.2.209 orclNWCongested

**Description**

Reserved for future use.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.160

**Other**

Single-valued attribute.

## 8.2.210 orclNrwTimeout

**Description**

Stores the network read/write time out. When an LDAP client initiates an operation, then does not respond to the server for a configured number of seconds, the server closes the connection. The number of seconds is controlled by the attribute `orclnrwtimeout` in the DSA configuration entry. The default is 300 seconds.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.603

**Other**

Single-valued attribute.

**8.2.211 orclNwUnavailable****Description**

Reserved for future use.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.159

**Other**

Single-valued attribute.

**8.2.212 orclObjectGUID****Description**

Stores Microsoft Active Directory's OBJECTGUID attribute value for users and groups migrated to Oracle Internet Directory from Active Directory.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.901

**Other**

Single-valued attribute.

**8.2.213 orclObjectSID****Description**

Stores Microsoft Active Directory's OBJECTSID attribute value for users and groups migrated to Oracle Internet Directory from Active Directory.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.902

**Other**

Single-valued attribute.

## 8.2.214 orclODIPAgent

**Description**

The DN of a provisioning profile.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch, caseIgnoreSubStringsMatch

**Object ID**

2.16.840.1.113894.9.1.6

## 8.2.215 orclODIPAgentConfigInfo

**Description**

Any configuration information that you want the connector to store in Oracle Internet Directory. It is passed by the Directory Integration Platform server to the connector at time of connector invocation. The information is stored as an attribute and the Directory Integration Platform server does not have any knowledge of its content. When the connector is scheduled for execution, the value of the attribute is stored in the file, `ORACLE_HOME/ldap/odi/conf/profile_name.cfg` that can be processed by the connector.

Upload the file by using:

```
manageSyncProfiles update -h host -p port -D WLS_userid -profile profile_name  
-params "odip.profile.configfile ORACLE_HOME/ldap/odi/conf/profile_name.cfg"
```

or

```
manageSyncProfiles update -h host -p port -D WLS_userid -profile profile_name  
-file properties_file
```

where *properties\_file* specifies`odip.profile.configfile=ORACLE_HOME/ldap/odi/conf/profile_name.cfg`.

Do this for both import and export agents.

See [Chapter 5, "Oracle Directory Integration Platform Tools"](#) and the *Oracle Fusion Middleware Administrator's Guide for Oracle Directory Integration Platform* for more information

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.24

**8.2.216 orclODIPAgentControl****Description**

Whether a synchronization profile is enabled or disabled. Valid values are ENABLE or DISABLE. The default is DISABLE.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.3

**Other**

Single-valued attribute.

**8.2.217 orclODIPAgentExeCommand****Description**

The executable name and argument list used by the Directory Integration Platform server to invoke a connector. It can be passed as a command-line argument when the connector is invoked. For example, here is a command to invoke the Oracle HR connector:

```
odihragent OracleHRAgent connect=hrdb login=%orclodipConDirAccessAccount  
pass=%orclodipConDirAccessPassword date=%orclODIPLastSuccessfulExecutionTime
```

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.21

**Other**

Single-valued attribute.

## 8.2.218 orclODIPAgentHostName

### Description

The host name of the Oracle Directory Integration and Provisioning server where the synchronization profile is run.

### Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

### Matching Rule

caseIgnoreMatch

### Object ID

2.16.840.1.113894.8.1.5

### Other

Single-valued attribute.

## 8.2.219 orclODIPAgentName

### Description

The name of a third-party synchronization profile.

### Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

### Matching Rule

caseIgnoreMatch

### Object ID

2.16.840.1.113894.8.1.1

### Other

Single-valued attribute.

## 8.2.220 orclODIPAgentPassword

### Description

Password that the synchronization profile uses to bind to the directory.

### Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

### Matching Rule

caseIgnoreMatch

### Object ID

2.16.840.1.113894.8.1.4

**Other**

Single-valued attribute.

**8.2.221 orclODIPApplicationName****Description**

The name of an application to which a provisioning subscription belongs.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch, caseIgnoreSubStringsMatch

**Object ID**

2.16.840.1.113894.9.1.7

**8.2.222 orclODIPApplicationsLocation****Description**

The DN of the application to which a provisioning subscription belongs.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.918

**Other**

Single-valued attribute.

**8.2.223 orclODIPAttributeMappingRules****Description**

Attribute for storing the mapping rules used by a synchronization profile. Store the mapping rules in a file by using the Directory Integration Platform Assistant. See [Chapter 5, "Oracle Directory Integration Platform Tools"](#) and the *Oracle Fusion Middleware Administrator's Guide for Oracle Directory Integration Platform* for more information about mapping rules.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.41

**8.2.224 orclODIPBootStrapStatus****Description**

The bootstrap status of a synchronization profile (the initial migration of data between a connected directory and Oracle Internet Directory).

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.101

**Other**

Single-valued attribute.

**8.2.225 orclODIPCommand****Description**

The command to invoke a provisioning profile.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.9.1.5

**8.2.226 orclODIPConDirAccessAccount****Description**

Valid user account in the connected directory to be used by the connector for synchronization. The value is specific to the connected directory with which you are integrating. For instance, for the SunONE synchronization connector, it is the valid bind DN in the SunONE Directory Server. For the Human Resources Connector, it is a valid user identifier in the Oracle Human Resources database. For other connectors, it can be passed as a command-line argument when the connector is invoked.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)



**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.22

**Other**

Single-valued attribute.

**8.2.227 orclODIPConDirAccessPassword****Description**

Password to be used by the user specified in the [orclODIPConDirAccessAccount](#) attribute to connect to the connected directory. The value is specific to the third-party directory with which you are integrating. For instance, for the SunONE synchronization connector, it is the valid bind password in the SunONE Directory Server. For the Human Resources Agent, it is the Oracle Human Resources database password.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.23

**8.2.228 orclODIPConDirLastAppliedChgNum****Description**

For Oracle Directory Integration and Provisioning import operations, the last change from the connected directory that was applied to Oracle Internet Directory. The default value is 0. If you have used the Directory Integration Platform Assistant to bootstrap the connected directory, then this value is set automatically. See [Chapter 5, "Oracle Directory Integration Platform Tools"](#) and the *Oracle Fusion Middleware Administrator's Guide for Oracle Directory Integration Platform* for more information about the bootstrap operation. This is valid only in the import profile.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.65

**Other**

Single-valued attribute.

## 8.2.229 orclODIPConDirMatchingFilter

### Description

This attribute specifies the filter to apply to the third-party directory change log. It is used in the Oracle Directory Integration and Provisioning import profile. The filter must be set in the import profile when both the import and export integration profiles are enabled, as follows:

```
Modifiersname != connected_directory_account
```

This prevents the same change from being exchanged between the two directories indefinitely. To avoid confusion, make this account specific to synchronization.

See Also: Note 280474.1, "Setting Up Filtering in a DIP Synchronization Profile" available at My Oracle Support (formerly MetaLink) at <http://metalink.oracle.com/>.

### Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

### Matching Rule

caseIgnoreMatch

### Object ID

2.16.840.1.113894.8.1.42

## 8.2.230 orclODIPConDirURL

### Description

Connection string required to connect to the third-party connected directory. This value refers to the host name and port number as *host:port:[sslmode]*.

To connect by using SSL, enter *host:port:1*.

Make sure the certificate to connect to the directory is stored in the wallet, the location of which is specified in the file *odi.properties*.

Note: To connect to SunONE Directory Server by using SSL, the server certificate needs to be loaded into the wallet.

See Also: The chapter on Oracle Wallet Manager in *Oracle Database Advanced Security Administrator's Guide*.

### Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

### Matching Rule

caseIgnoreMatch

### Object ID

2.16.840.1.113894.8.1.25

### Other

Single-valued attribute.

## 8.2.231 orclODIPConfigDNs

### Description

Stores the DN's of integration profiles for a particular configuration set in Oracle Directory Integration Platform.

### Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

### Matching Rule

caseIgnoreMatch

### Object ID

2.16.840.1.113894.8.1.72

## 8.2.232 orclODIPConfigRefreshFlag

### Description

Stores a flag which indicates whether any integration profiles have been added, deleted, or modified. Used in association with a configuration set.

### Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

### Matching Rule

caseIgnoreMatch

### Object ID

2.16.840.1.113894.8.1.71

### Other

Single-valued attribute.

## 8.2.233 orclODIPDbConnectInfo

### Description

The connection string for the database of a provisioning profile subscriber. The format of the string is host:port:sid:username:password.

### Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

### Matching Rule

caseIgnoreMatch, caseIgnoreSubStringsMatch

### Object ID

2.16.840.1.113894.9.1.2

## 8.2.234 orclODIPEncryptedAttrKey

### Description

Stores a key which is used to encrypt and decrypt sensitive data that is transmitted by the Oracle directory integration platform server to other applications.

### Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

### Matching Rule

caseIgnoreMatch

### Object ID

2.16.840.1.113894.8.1.215

### Other

Single-valued attribute.

## 8.2.235 orclODIPEventFilter

### Description

Reserved for future use.

### Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

### Matching Rule

caseIgnoreMatch

### Object ID

2.16.840.1.113894.8.1.433

## 8.2.236 orclODIPEventSubscriptions

### Description

Store configuration information for events to which a provisioned-integrated application subscribes.

### Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

### Matching Rule

caseIgnoreMatch, caseIgnoreSubStringsMatch

### Object ID

2.16.840.1.113894.9.1.1

## 8.2.237 orclODIPFilterAttrCriteria

**Description**

Reserved for future use.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.605

**Other**

Single-valued attribute.

## 8.2.238 orclODIPInstancesLocation

**Description**

Identifies the location in the directory that stores information about instances of the Oracle directory integration platform server.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.913

**Other**

Single-valued attribute.

## 8.2.239 orclODIPInstanceStatus

**Description**

Stores a flag that indicates whether an instance of the Oracle directory integration platform server should continue running or shut down. This flag provides a means of communication between the OID Monitor, OID Control, and the Oracle directory integration platform server.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.76

**Other**

Single-valued attribute.

**8.2.240 orclODIPIInterfaceType****Description**

The data format or protocol used in synchronization with a third-party directory. Supported values are:

- LDIF—Import or export from a LDIF File.
- Tagged—Import or export from a tagged file—a proprietary format supported by the Oracle Directory Integration Platform server, similar to LDIF format.
- LDAP—Import from or export to an LDAP-compliant directory.
- DB —Import from or export to an Oracle Database directory.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.28

**Other**

Single-valued attribute.

**8.2.241 orclODIPLastExecutionTime****Description**

Status attribute set to the last time the integration profile was executed by the Oracle Directory Integration and Provisioning server. Its format is dd-mon-yyyy hh:mm:ss, where hh is the time of day in 24-hour format. This attribute is initialized during profile creation.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.61

**Other**

Single-valued attribute.

## 8.2.242 orclODIPLastSuccessfulExecutionTime

### Description

Status attribute set to the last time the integration profile was executed successfully by the Oracle Directory Integration and Provisioning server. Its format is `dd-mon-yyyy hh:mm:ss`, where `hh` is the time of day in 24-hour format. This attribute is initialized during profile creation.

### Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

### Matching Rule

caseIgnoreMatch

### Object ID

2.16.840.1.113894.8.1.62

### Other

Single-valued attribute.

## 8.2.243 orclODIPMustAttrCriteria

### Description

Reserved for future use.

### Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

### Matching Rule

caseIgnoreMatch

### Object ID

2.16.840.1.113894.8.1.603

### Other

Single-valued attribute.

## 8.2.244 orclODIObjectCriteria

### Description

Used in an object definition to identify and classify a particular type of object.

### Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

### Matching Rule

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.602

## 8.2.245 orclODIPObjectDefnLocation

**Description**

Identifies the location of the various object definitions used by the Oracle directory integration platform server.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.917

**Other**

Single-valued attribute.

## 8.2.246 orclODIPObjectEvents

**Description**

Reserved for future use.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.432

## 8.2.247 orclODIPObjectName

**Description**

Used in an object definition to store the name of an object.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.601



**Other**

Single-valued attribute.

**8.2.248 orclODIObjectSyncBase****Description**

The search base in the directory for an object associated with an Oracle Directory Integration and Provisioning synchronization profile.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.431

**8.2.249 orclODIROIDMatchingFilter****Description**

In export profiles, this attribute specifies the filter to apply to the Oracle Internet Directory change log container. It is used in the export profile. It must be set in the export profile when both the import and export integration profiles are enabled, as in the following example:

```
Modifiersname !=orclodipagentname=iPlanetImport,cn=subscriber profile,cn=changelog  
subscriber,cn=oracle internet directory
```

This prevents the same change from being exchanged between the two directories indefinitely.

In import profiles, this attribute specifies a key for mapping entries between Oracle Internet Directory and the connected directory. This is useful when the DN cannot be used as the key.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.43

**8.2.250 orclODIOperationMode****Description**

Reserved for future use.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.430

## 8.2.251 orclODIPOptAttrCriteria

**Description**

Reserved for future use.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.604

**Other**

Single-valued attribute.

## 8.2.252 orclODIPPluginAddInfo

**Description**

Additional information that may be needed by an Oracle Directory Integration and Provisioning connector plug-in.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.264

**Other**

Single-valued attribute.

## 8.2.253 orclODIPPluginConfigInfo

**Description**

Reserved for future use.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.261

**Other**

Single-valued attribute.

**8.2.254 orclODIPPluginEvents****Description**

Reserved for future use.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.265

**8.2.255 orclODIPPluginExecData****Description**

The Oracle Directory Integration and Provisioning connector plug-in executable data, which is typically a JAR file.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.5 (Binary Data)

**Matching Rule**

N/A

**Object ID**

2.16.840.1.113894.8.1.262

**8.2.256 orclODIPPluginExecName****Description**

The fully qualified name of the Oracle Directory Integration and Provisioning connector plug-in executable, which is typically a Java class.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.263

**Other**

Single-valued attribute.

## 8.2.257 orclODIPProfileDataLocation

**Description**

Reserved for future use.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.914

**Other**

Single-valued attribute.

## 8.2.258 orclODIPProfileDebugLevel

**Description**

The debugging level for an Oracle Directory Integration and Provisioning synchronization profile.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.251

**Other**

Single-valued attribute.

---

---

**Note:** To log all information for a synchronization profile, including entries that are synchronized, set the `orclODIPProfileDebugLevel` to a value of 63 for 10g and to a value of 64 for 11g.

The `orclodipprofiledebuglevel` attribute corresponds to the `odip.profile.debuglevel` configuration property. The `odip.profile.debuglevel` property refers to the following log levels, which you can set in the Oracle Enterprise Manager Fusion Middleware Control by editing the **Log Level** under the **Advanced** tab:

- Off = 0
  - Error = 8
  - Info = 16
  - Trace = 32
  - All = 64 (recommended for most sync/profile mapping troubleshooting)
- 
- 

## 8.2.259 orclODIPProfileExecGroupID

### Description

Associates a group number with a particular provisioning profile.

### Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

### Matching Rule

caseIgnoreMatch

### Object ID

2.16.840.1.113894.8.1.250

### Other

Single-valued attribute.

## 8.2.260 orclODIPProfileInterfaceAdditionalInformation

### Description

Reserved for future use.

### Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

### Matching Rule

caseIgnoreMatch

### Object ID

2.16.840.1.113894.8.1.223

## 8.2.261 orclODIPProfileInterfaceConnectInformation

**Description**

Contains information that is used by the Oracle directory integration platform server on how to connect to a provisioning-integrated application for event propagation.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.222

**Other**

Single-valued attribute.

## 8.2.262 orclODIPProfileInterfaceName

**Description**

Contains a provisioning-integrated application's interface name, which is used by the Oracle directory integration platform server for event propagation. The value assigned to this attribute depends on the interface type.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.220

**Other**

Single-valued attribute.

## 8.2.263 orclODIPProfileInterfaceType

**Description**

Specifies the type of interface to which events is propagated by the Oracle directory integration platform server. Valid values for this attribute are PLSQL or JAVA.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.221

**Other**

Single-valued attribute.

**8.2.264 orclODIPProfileInterfaceVersion****Description**

Specifies the provisioning profile version to which events is propagated by the Oracle directory integration platform server.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.224

**Other**

Single-valued attribute.

**8.2.265 orclODIPProfileLastAppliedAppEventID****Description**

Contains the number of the last event that was generated by a provisioning-integration application and updated in Oracle Internet Directory by the Oracle directory integration platform server.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.234

**Other**

Single-valued attribute.

**8.2.266 orclODIPProfileLastProcessingTime****Description**

The last time the Oracle Directory Integration and Provisioning synchronization profile was executed.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.232

**Other**

Single-valued attribute.

## 8.2.267 orclODIPProfileLastSuccessfulProcessingTime

**Description**

The last time the Oracle Directory Integration and Provisioning synchronization profile was successfully executed.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.233

**Other**

Single-valued attribute.

## 8.2.268 orclODIPProfileMaxErrors

**Description**

Reserved for future use.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.214

**Other**

Single-valued attribute.



## 8.2.269 orclODIPProfileMaxEventsPerInvocation

### Description

Specifies the maximum number of events that the Oracle directory integration platform server packages and sends to an application during one invocation of a provisioning profile.

### Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

### Matching Rule

caseIgnoreMatch

### Object ID

2.16.840.1.113894.8.1.212

### Other

Single-valued attribute.

## 8.2.270 orclODIPProfileMaxEventsPerSchedule

### Description

Specifies the maximum number of events that the Oracle directory integration platform server sends to an application during one execution of a provisioning profile.

### Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

### Matching Rule

caseIgnoreMatch

### Object ID

2.16.840.1.113894.8.1.213

### Other

Single-valued attribute.

## 8.2.271 orclODIPProfileMaxRetries

### Description

The maximum number of times an Oracle Directory Integration and Provisioning profile is retried in the event of an error.

### Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

### Matching Rule

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.211

**Other**

Single-valued attribute.

## 8.2.272 orclODIPProfileName

**Description**

The name of the Oracle Directory Integration and Provisioning profile.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.201

**Other**

Single-valued attribute.

## 8.2.273 orclODIPProfileProcessingErrors

**Description**

Contains errors raised during event propagation by the Oracle directory integration platform server for a particular provisioning-integrated application.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.231

## 8.2.274 orclODIPProfileProcessingStatus

**Description**

Contains the Oracle directory integration platform server's event propagation status for a particular provisioning-integrated application.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.230

**Other**

Single-valued attribute.

**8.2.275 orclODIPProfileProvSubscriptionMode****Description**

The subscription mode for a provisioning profile: INBOUND, OUTBOUND, or BOTH.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.408

**8.2.276 orclODIPProfileSchedule****Description**

The number of seconds between executions of an Oracle Directory Integration and Provisioning profile. The default is 3600, which means the profile is scheduled to run every hour.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.210

**Other**

Single-valued attribute.

**8.2.277 orclODIPProfileStatusUpdate****Description**

Indicates whether the Oracle directory integration platform server should perform a provisioning profile status update while propagating events to a provisioning-integrated application.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.610

**Other**

Single-valued attribute.

**8.2.278 orclODIPProvEventCriteria****Description**

Used with version 2.0 provisioning profiles to convert a change in Oracle Internet Directory to an event before propagating it to a provisioning-integrated application. This attribute is used to identify a particular type of event.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.503

**8.2.279 orclODIPProvEventLDAPChangeType****Description**

Used with version 2.0 provisioning profiles to convert a change in Oracle Internet Directory to an event before propagating it to a provisioning-integrated application. This attribute is used to indicate what type of operation in LDAP (add, modify, delete) can cause some type of event.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.502

**8.2.280 orclODIPProvEventObjectType****Description**

Used with version 2.0 provisioning profiles to convert a change in Oracle Internet Directory to an event before propagating it to a provisioning-integrated application. This attribute is used to indicate the type of object (i.e whether it is a USER or a GROUP and so forth) based on other qualifying criteria.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.501

**Other**

Single-valued attribute.

## 8.2.281 orclODIPProvEventRule

**Description**

Stores the XML-based rule definitions used by the Oracle directory integration platform server to convert changes in Oracle Internet Directory into events before propagating them to a provisioning-integrated application.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.607

**Other**

Single-valued attribute.

## 8.2.282 orclODIPProvEventRuleDTD

**Description**

Stores the XML DTD for event rule definitions used by the Oracle directory integration platform server to understand and parse event rule definitions.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.606

**Other**

Single-valued attribute.

## 8.2.283 orclODIPProvInterfaceFilter

### Description

Used with version 3.0 provisioning profiles to identify and classify an object based on the entry's object class. This attribute is used in the object definitions stored in Oracle Internet Directory.

### Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

### Matching Rule

caseIgnoreMatch

### Object ID

2.16.840.1.113894.8.1.609

## 8.2.284 orclODIPProvInterfaceProcessor

### Description

Used by the Oracle directory integration platform server to identify the Java classes to use for reading and writing events from and to provisioning-integration applications and for processing event propagation results. The default configurations in this attribute should not be changed.

### Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

### Matching Rule

caseIgnoreMatch

### Object ID

2.16.840.1.113894.8.1.608

### Other

Single-valued attribute.

## 8.2.285 orclODIPProvisioningAppGUID

### Description

The global unique identifier for the application entry associated with a provisioning profile.

### Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

### Matching Rule

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.402

**Other**

Single-valued attribute.

**8.2.286 orclODIPProvisioningAppName****Description**

The distinguished name (DN) of the application to which the provisioning subscription belongs. The combination of the application name and organization name uniquely identifies a provisioning profile, for example, Email.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.401

**Other**

Single-valued attribute.

**8.2.287 orclODIPProvisioningEventMappingRules****Description**

The event mapping rule maps the object type received from the application (using an optional filter condition) to a domain in Oracle Internet Directory. An inbound provisioning profile can have multiple mapping rules defined.

The following example shows a sample mapping rule value. The rule shows that a user object (USER) whose locality attribute equals US (l=US) should be mapped to the domain l=US, cn=users, dc=company, dc=com.

```
USER:l=US:l=US, cn=users, dc=company, dc=com
```

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.406

## 8.2.288 orclODIPProvisioningEventPermittedOperations

### Description

Defines the types of events that the application is allowed to send to the Oracle Directory Integration and Provisioning service. An inbound provisioning profile can have multiple permitted operations defined.

For example, if you wanted to permit the application to send events whenever a user object was added or deleted, or when certain attributes were modified, you would have three permitted operation values such as this:

```
USER:dc=mycompany,dc=com:ADD(*)
USER:dc=mycompany,dc=com:MODIFY(cn,sn,mail,password)
USER:dc=mycompany,dc=com:DELETE(*)
```

### Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

### Matching Rule

caseIgnoreMatch

### Object ID

2.16.840.1.113894.8.1.407

## 8.2.289 orclODIPProvisioningEventSubscription

### Description

Defines the types of events that the Oracle Directory Integration and Provisioning service should send to the application. An outbound provisioning profile can have multiple event subscriptions defined.

For example, if you wanted the directory integration server to send events to the application whenever a user or group object was added or deleted, you would have four event subscription values such as this:

```
GROUP:dc=mycompany,dc=com:ADD(*)
GROUP:dc=mycompany,dc=com:DELETE(*)
USER:dc=mycompany,dc=com:ADD(*)
USER:dc=mycompany,dc=com:DELETE(*)
```

### Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

### Matching Rule

caseIgnoreMatch

### Object ID

2.16.840.1.113894.8.1.405



## 8.2.290 orclODIPProvisioningOrgGUID

**Description**

The global unique identifier for the organization entry associated with a provisioning profile.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.404

**Other**

Single-valued attribute.

## 8.2.291 orclODIPProvisioningOrgName

**Description**

The distinguished name (DN) of the organization to which the provisioning subscription belongs, for example `dc=company,dc=com`. The combination of the application DN and organization DN uniquely identifies a provisioning profile. Defaults value is the DN of the default identity management realm.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.403

**Other**

Single-valued attribute.

## 8.2.292 orclODIPProvProfileLocation

**Description**

Contains the DN of the directory container that stores provisioning profiles.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.916

**Other**

Single-valued attribute.

## 8.2.293 orclODIPRootLocation

**Description**

Refers to the root location in the directory tree where the Oracle Directory Integration Platform configuration is stored.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.912

**Other**

Single-valued attribute.

## 8.2.294 orclODIPSchedulingInterval

**Description**

Time interval in seconds after which a connected directory is synchronized with Oracle Internet Directory. The default is 600.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.6

**Other**

Single-valued attribute.

## 8.2.295 orclODIPSchemaVersion

**Description**

Reserved for future use.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.911

**Other**

Single-valued attribute.

**8.2.296 orclODIPSearchCountLimit****Description**

Reserved for future use.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.511

**Other**

Single-valued attribute.

**8.2.297 orclODIPSearchTimeLimit****Description**

Reserved for future use.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.512

**Other**

Single-valued attribute.

**8.2.298 orclODIPServerCommitSize****Description**

Reserved for future use.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.515

**Other**

Single-valued attribute.

## 8.2.299 orclODIPServerConfigLocation

**Description**

Reserved for future use.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.919

**Other**

Single-valued attribute.

## 8.2.300 orclODIPServerDebugLevel

**Description**

The number that corresponds to the debugging level for the Oracle Directory Integration and Provisioning server.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.516

**Other**

Single-valued attribute.

### 8.2.301 orclODIPServerRefreshIntvl

**Description**

The number of minutes between server refreshes for any changes in Oracle Directory Integration Platform profiles. If not specified, the default of 2 is used.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.514

**Other**

Single-valued attribute.

### 8.2.302 orclODIPServerSSLMode

**Description**

The number of the corresponding SSL mode. The default is 0. The modes are as follows:

- 0 — SSL is not used.
- 1 — SSL is used for encryption only, not for authentication.
- 2 — SSL is used for one-way authentication. With this mode you must also specify the complete path and file name of the server's Oracle Wallet.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.513

**Other**

Single-valued attribute.

### 8.2.303 orclODIPServerWalletLoc

**Description**

The complete path and file name of the Oracle Directory Integration and Provisioning server's Oracle Wallet.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.517

**Other**

Single-valued attribute.

## 8.2.304 orclODIPSynchronizationErrors

**Description**

Messages explaining the errors if the last execution of the synchronization profile failed. This attribute is updated by Oracle Directory Integration and Provisioning server.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.64

## 8.2.305 orclODIPSynchronizationMode

**Description**

Direction of synchronization between Oracle Internet Directory and the connected directory. Allowed values are: IMPORT or EXPORT.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.2

**Other**

Single-valued attribute.

## 8.2.306 orclODIPSynchronizationStatus

**Description**

Status of the last execution of a synchronization profile: SUCCESS or FAILURE. Initially, this attribute has the value YET TO BE EXECUTED.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.63

**Other**

Single-valued attribute.

### 8.2.307 orclODIPSyncProfileLocation

**Description**

Reserved for future use.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.915

**Other**

Single-valued attribute.

### 8.2.308 orclODIPSyncRetryCount

**Description**

Maximum number of times Oracle Directory Integration and Provisioning server tries to run the third-party directory connector in the event of a failure. The default is 5.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.7

**Other**

Single-valued attribute.

### 8.2.309 orclOidComponentName

**Description**

Name of OID component where replication server is started.

**Syntax**

Directory String

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.832

### 8.2.310 orclOidInstanceName

**Description**

Name of instance where replication server is started.

**Syntax**

Directory String

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.830

### 8.2.311 orclOpAbandoned

**Description**

Specifies the number of abandoned LDAP operations.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.168

**Other**

Single-valued attribute.



## 8.2.312 orclOpCompleted

**Description**

Specifies the number of completed LDAP operations.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.166

**Other**

Single-valued attribute.

## 8.2.313 orclOpenConn

**Description**

Specifies the number of open connections to the Oracle Internet Directory server, including client LDAP connections and database connections.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.149

**Other**

Single-valued attribute.

## 8.2.314 orclOpFailed

**Description**

Specifies the number of failed LDAP operations.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.190

**Other**

Single-valued attribute.

## 8.2.315 orclOpInitiated

**Description**

Specifies the number of initiated LDAP operations.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.165

**Other**

Single-valued attribute.

## 8.2.316 orclOpLatency

**Description**

Stores operation latency.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.127

**Other**

Single-valued attribute.

## 8.2.317 orclOpPending

**Description**

Specifies the number of pending LDAP operations.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.167

**Other**

Single-valued attribute.

**8.2.318 orclOpResult****Description**

Stores the operation result.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.64

**8.2.319 orclOpSucceeded****Description**

Specifies the number of successful LDAP operations.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.189

**Other**

Single-valued attribute.

**8.2.320 orclOpTimedOut****Description**

Specifies the number of LDAP search operations that timed out.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.169

**Other**

Single-valued attribute.

**8.2.321 orcloptracklevel****Description**

Security event tracking level.

**Syntax**

Integer

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.180

**8.2.322 orcloptrackmaxtotalsize****Description**

Maximum number of bytes of RAM that security events tracking can use for each type of operation.

**Syntax**

Integer

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.178

**8.2.323 orcloptracknumelemcontainers****Description**

Number of in-memory cache containers to be allocated for security event tracking. The `1stlevel` subtype is for setting the number of in-memory cache containers for storing information about users performing operations. The `2ndlevel` subtype, which is applicable only to compare operation, sets the number of in-memory cache containers for information about the users whose userpassword is compared and tracked when detailed compare operation statistics is programmed.

**Syntax**

Integer

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.181

**8.2.324 orclORA28error****Description**

Specifies the number of ORA-28 errors encountered by Oracle Internet Directory server.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.182

**Other**

Single-valued attribute.

**8.2.325 orclORA3113error****Description**

Specifies the number of ORA-3113 errors encountered by Oracle Internet Directory server.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.157

**Other**

Single-valued attribute.

**8.2.326 orclORA3114error****Description**

Specifies the number of ORA-3114 errors encountered by Oracle Internet Directory server.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.158

**Other**

Single-valued attribute.

## 8.2.327 orclOracleHome

**Description**

The *ORACLE\_HOME* location of an Oracle service.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

N/A

**Object ID**

2.16.840.1.113894.7.1.2

**Other**

Single-valued attribute.

## 8.2.328 orclOwnerGUID

**Description**

The global unique identifier of the user who owns an application or resource.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch, caseIgnoreSubstringsMatch

**Object ID**

2.16.840.1.113894.1.1.358

## 8.2.329 orclPassword

**Description**

Identifies an Oracle-specific password for custom authentication schemes like O3Logon for the database server.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.44 (Printable String)

**Matching Rule**

caseExactMatch

**Object ID**

2.16.840.1.113894.7.1.13

**8.2.330 orclPasswordAttribute****Description**

Specifies the password value to access the resource.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch, caseIgnoreSubstringsMatch

**Object ID**

2.16.840.1.113894.1.1.353

**Other**

Single-valued attribute.

**8.2.331 orclPasswordHint****Description**

Specifies the password hint to be displayed when users forget their password.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.314

**Other**

Single-valued attribute.

**8.2.332 orclPasswordHintAnswer****Description**

The answer related to the password hint question stored in [orclPasswordHint](#).

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.315

**Other**

Single-valued attribute.

---

---

**Note:** `orclPasswordHintAnswer` is hashed using the SHA-1 algorithm. The hexadecimal value of this is Base64 encoded.

Oracle Internet Directory hashes the value only if it is provided as plaintext. Prehashed values are not hashed again.

---

---

### 8.2.333 orclPasswordVerifier

**Description**

Attribute for storing a password to an Oracle component when that password is different from that used to authenticate the user to the directory, namely, `userPassword`. The value in this attribute is not synchronized with that in the `userPassword` attribute.

Like `authPassword`, this attribute is multivalued and can contain all the other verifiers that different applications use for this user's clear text password.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.44{128} (Printable String, 128 character maximum)

**Matching Rule**

octetStringMatch

**Object ID**

2.16.840.1.113894.1.1.210

### 8.2.334 orclPilotMode

**Description**

Whether to BEGIN or END pilot mode for a replica.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Directory String)

**Matching Rule**

caseIgnoreMatch, caseIgnoreSubstringsMatch, equality integermatch



**Object ID**

2.16.840.1.113894.1.1.824

**Other**

Single-valued attribute.

**8.2.335 orclPKCS12Hint****Description**

Password hint for the user's PKCS12 private key store.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.7.1.11

**8.2.336 orclPKIMatchingRule****Description**

This is used to specify the matching rule for mapping a user's PKI certificate DN to the user's entry DN in Oracle Internet Directory. The following matching rule values are allowed:

- 0 - Exact match. The PKI certificate DN must match the user entry DN.
- 1 - Certificate search. Check to see if the user has a PKI certificate provisioned into Oracle Internet Directory.
- 2 - A combination of exact match and certificate search. If the exact match fails, then a certificate search is performed.
- 3 - Mapping rule only. Use a mapping rule to map user PKI certificate DN to Oracle Internet Directory DN.
- 4 - Try in order: 1 (mapping rule), 2 (certificate search), 3 (exact match).

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.703

**Other**

Single-valued attribute.

### 8.2.337 orclPKINextUpdate

**Description**

The universal time when the certificate revocation list (CRL) should be updated.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.53 (UTC Time)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.2.1.300.1

### 8.2.338 orclPKIVaIMecAttr

**Description**

Contains the certificate validation mechanism supported. Currently, only validation with crls is supported, hence the value of this attribute is CRL.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.2.1.300.2

### 8.2.339 orclPluginAttributeList

**Description**

A semicolon-separated attribute name list that controls whether the plug-in takes effect. If the target attribute is included in the list, the plug-in is invoked.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.563

**Other**

Single-valued attribute.

## 8.2.340 orclPluginCheckEntryExist

### Description

If enabled, then the Plug-in is invoked when the base entry does not exist. This only applies to search operation with scope base.

Allowed values are 0 (disabled) or 1 (enabled).

### Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

### Matching Rule

caseIgnoreMatch

### Object ID

2.16.840.1.113894.1.1.569

### Other

Single-valued attribute.

## 8.2.341 orclPluginEnable

### Description

Whether a plug-in is enabled or disabled. Allowed values are 0 (disabled) or 1 (enabled). The default is 0 (disabled).

### Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

### Matching Rule

caseIgnoreMatch

### Object ID

2.16.840.1.113894.1.1.554

### Other

Single-valued attribute.

## 8.2.342 orclPluginEntryProperties

### Description

An LDAP search filter that specifies entry criteria that will cause the plug-in to not be invoked. For example, if the following filter is used, the plug-in will not be invoked if the target entry has objectclass equal to inetorgperson and sn equal to Cezanne.

```
(&(objectclass=inetorgperson)(sn=Cezanne))
```

### Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.568

**Other**

Single-valued attribute.

## 8.2.343 orclPluginIsReplace

**Description**

For plug-ins that use WHEN timing only. 0 is disabled (default). 1 is enabled. This attribute can be set to enabled only if the `orclPluginLDAPOperation` attribute value is `ldapbind`, `ldapcompare`, or `ldapmodify`.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.559

**Other**

Single-valued attribute.

## 8.2.344 orclPluginBinaryFlexfield

**Description**

Custom binary information (Java only)

**Syntax**

1.3.6.1.4.1.1466.115.121.1.5

**Object ID**

2.16.840.1.113894.1.1.574

**Other**

Single-valued attribute.

## 8.2.345 orclPluginFlexfield

**Description**

Custom text information (Java only). To indicate a subtype, specify `orclPluginFlexfield; subtypeName`, for example, `orclPluginFlexfield; minPwdLength: 8`

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.573

**Other**

Single-Valued attribute.

**8.2.346 orclPluginSecuredFlexfield****Description****Syntax**

1.3.6.1.4.1.1466.115.121.1.15

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.577

**Other**

Single-Valued attribute.

**8.2.347 orclPluginKind****Description**

The kind of plug-in. PL/SQL is the only allowed value.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.562

**Other**

Single-valued attribute.

## 8.2.348 orclPluginLDAPOperation

**Description**

The LDAP operation that this plug-in supplements. Allowed values are:

- ldapcompare
- ldapmodify
- ldapbind
- ldapadd
- ldapdelete
- ldapsearch

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.557

**Other**

Single-valued attribute.

## 8.2.349 orclPluginName

**Description**

The plug-in package name.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.552

**Other**

Single-valued attribute.

## 8.2.350 orclPluginPort

**Description**

The port that the plug-in is using.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.566

**Other**

Single-valued attribute.

## 8.2.351 orclPluginRequestGroup

**Description**

A semicolon-separated group list that controls if the plug-in takes effect. You can use this group to specify who can actually invoke the plug-in. For example, if you specify `orclpluginrequestgroup:cn=security,cn=groups,dc=oracle,dc=com`, when you register the plug-in, then the plug-in will not be invoked unless the ldap request comes from the person who belongs to the group `cn=security,cn=groups,dc=oracle,dc=com`.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.564

**Other**

Single-valued attribute.

## 8.2.352 orclPluginRequestNegGroup

**Description**

A semicolon-separated group list that controls if the plug-in takes effect. You can use this group to specify who cannot invoke the plug-in. For example, if you specify `orclpluginrequestneggroup:cn=security,cn=groups,dc=oracle,dc=com`, when you register the plug-in, then the plug-in will not be invoked if the ldap request comes from the person who belongs to the group `cn=security,cn=groups,dc=oracle,dc=com`.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.571

**Other**

Single-valued attribute.

**8.2.353 orclPluginResultCode****Description**

An integer value to specify the LDAP result code. If this value is specified, then the plug-in is invoked only if the ldap operation is in that result code scenario. This only applies if the value for the [orclPluginTiming](#) attribute is POST.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.565

**Other**

Single-valued attribute.

**8.2.354 orclPluginSASLCallback****Description**

Controls the type of bind used when the LDAP\_PLUGIN package connects back to the same Oracle Internet Directory server.

- 1= SASL bind (default).
- 0= Simple bind.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.572

**Other**

Single-valued attribute.



## 8.2.355 orclPluginSearchNotFound

### Description

This only applies if the value for the [orclPluginTiming](#) attribute is `POST`. Brings in the external entries if the entry is not found in Oracle Internet Directory. Provides additional plug-in invocation checking and ensures that the plug-in will only be invoked when the entry is not present in Oracle Internet Directory.

### Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

### Matching Rule

caseIgnoreMatch

### Object ID

2.16.840.1.113894.1.1.570

### Other

Single-valued attribute.

## 8.2.356 orclPluginShareLibLocation

### Description

File location of the program libraries for the plug-in. If this value is not present, then the Oracle Internet Directory server assumes the plug-in language is PL/SQL.

### Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

### Matching Rule

caseIgnoreMatch

### Object ID

2.16.840.1.113894.1.1.556

### Other

Single-valued attribute.

## 8.2.357 orclPluginSubscriberDNList

### Description

A semicolon-separated DN list that controls if the plug-in takes effect. For example:

```
dc=COM, c=us ; dc=us, dc=oracle, dc=com ; dc=org, dc=us ; o=IMC, c=US
```

If the target DN of an LDAP operation is included in the list, then the plug-in is invoked.

### Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.561

**Other**

Single-valued attribute.

**8.2.358 orclPluginTiming****Description**

Specifies when the plug-in is to be invoked in relation to the LDAP operation it supplements. The following values are allowed:

- PRE
- WHEN
- POST

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.558

**Other**

Single-valued attribute.

**8.2.359 orclPluginType****Description**

Valid value is *operational* — Operational plug-ins augment existing LDAP operations. The work they perform depends on whether they execute before, after, or in addition to normal directory server operations.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.553

**Other**

Single-valued attribute.

## 8.2.360 orclPluginVersion

**Description**

The supported version number of the plug-in.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.555

**Other**

Single-valued attribute.

## 8.2.361 OrclPluginWorkers

**Description**

Number of plug-in threads per server process.

**Syntax**

Integer

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.612

## 8.2.362 orclPrName

**Description**

Stores a process name.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

**Matching Rule**

distinguishedNameMatch

**Object ID**

2.16.840.1.113894.1.1.55

**Other**

Single-valued attribute.

## 8.2.363 orclProductVersion

### Description

Identifies the product version.

### Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

### Matching Rule

caseIgnoreMatch

### Object ID

2.16.840.1.113894.7.1.6

## 8.2.364 orclPrPassword

### Description

Contains a password for the OID proxy user.

### Syntax

1.3.6.1.4.1.1466.115.121.1.15{128} (Directory String, 128 character maximum)

### Matching Rule

caseIgnoreMatch, caseIgnoreSubstringsMatch

### Object ID

2.16.840.1.113894.1.1.56

### Other

Single-valued attribute.

## 8.2.365 orclPurgeBase

### Description

The base DN in the directory information tree (DIT) where the garbage collection task is applied. This attribute value is reserved for each garbage collector and it must not be modified. Defaults to the RDN of the garbage collector configuration entry DN.

### Syntax

1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

### Matching Rule

distinguishedNameMatch

### Object ID

2.16.840.1.113894.1.1.805

### Other

Single-valued attribute.

## 8.2.366 orclPurgeDebug

**Description**

Flag to enable (1) or disable (0) collection of debugging messages. Default value is 0.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.810

**Other**

Single-valued attribute.

## 8.2.367 orclPurgeEnable

**Description**

Flag to enable (1) or disable (0) this garbage collector. Default value is 1.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch, caseIgnoreSubstringsMatch

**Object ID**

2.16.840.1.113894.1.1.808

**Other**

Single-valued attribute.

## 8.2.368 orclPurgeFileLoc

**Description**

Absolute file directory where the garbage collection log file is saved. Default value is . (period - the current directory).

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch, caseIgnoreSubstringsMatch

**Object ID**

2.16.840.1.113894.1.1.812

**Other**

Single-valued attribute.

## 8.2.369 orclPurgeFileName

**Description**

The file name of the garbage collection log file. Default value is `oidgc001.log`.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

`caseIgnoreMatch`, `caseIgnoreSubstringsMatch`

**Object ID**

2.16.840.1.113894.1.1.811

**Other**

Single-valued attribute.

## 8.2.370 orclPurgeFilter

**Description**

Reserved for future use.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

`caseIgnoreMatch`, `caseIgnoreSubstringsMatch`

**Object ID**

2.16.840.1.113894.1.1.803

**Other**

Single-valued attribute.

## 8.2.371 orclPurgeInterval

**Description**

Time interval in hours that the garbage collection job is executed again. This can be measured from either the point in time specified in the `orclPurgeStart` attribute or from the last time it was run. Default value is 24.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

`integerMatch`

**Object ID**

2.16.840.1.113894.1.1.801

**Other**

Single-valued attribute.

**8.2.372 orclPurgeNow****Description**

Every time this attribute is added or modified to a garbage collection entry, then the submitted job is executed immediately.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch, caseIgnoreSubstringsMatch

**Object ID**

2.16.840.1.113894.1.1.809

**Other**

Single-valued attribute.

**8.2.373 orclPurgePackage****Description**

Specifies the package name for purging directory objects.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch, caseIgnoreSubstringsMatch

**Object ID**

2.16.840.1.113894.1.1.804

**Other**

Single-valued attribute.

**8.2.374 orclPurgeSchedule****Description**

Specifies the schedule for purging directory objects.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integermatch

**Object ID**

2.16.840.1.113894.1.1.24

**Other**

Single-valued attribute.

DSA operational attribute.

**8.2.375 orclPurgeStart****Description**

The time when the garbage collector starts to run. The format is `yyyymmddhhmmss`. Default value is 12:00 a.m. of the day Oracle Internet Directory is installed.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch, caseIgnoreSubstringsMatch

**Object ID**

2.16.840.1.113894.1.1.813

**Other**

Single-valued attribute.

**8.2.376 orclPurgeTargetAge****Description**

This attribute enables time-based purging of change log records. Set this to the number of hours after which old change logs are purged. Time-based purging respects the change status of replication, but not the change status of other consumers. When time-based purging is enabled, the change log garbage collector purges all change logs that are not needed by replication and that are at least the specified number of hours old.

The default behavior is change number-based purging, meaning this attribute is NULL or set to a value less than zero. Change number-based purging respects the change status of all change log consumers. That is, it does not purge change logs unless they have been consumed by all consumers. In addition, it does not purge change logs until they are 10 days old.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch



**Object ID**

2.16.840.1.113894.1.1.800

**Other**

Single-valued attribute.

**8.2.377 orclPurgeTranSize****Description**

The number of objects to be purged in one commit transaction. The default value is 1000.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.802

**Other**

Single-valued attribute.

**8.2.378 orclPwdAccountUnlock****Description**

It allows a user with the appropriate administration rights and privileges to unlock an already locked account. However, it doesn't necessarily imply that the user affected (that is, who's account was locked) can unlock it by changing this attribute.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

**Matching Rule**

booleanMatch

**Object ID**

2.16.840.1.113894.1.1.203

**Other**

Single-valued attribute.

**8.2.379 orclPwdAllowHashCompare****Description**

Whether to allow password validations by comparing the hash values of encrypted passwords. Allowed values are TRUE or FALSE.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

**Matching Rule**

booleanMatch

**Object ID**

2.16.840.1.113894.1.1.218

**Other**

Single-valued attribute.

## 8.2.380 orclPwAlphaNumeric

**Description**

Number of numeric characters required in a password. The default value is 1.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.205

**Other**

Single-valued attribute.

## 8.2.381 orclPwEncryptionEnable

**Description**

If the value is 1, then the user password is stored in reversible encrypted form. If the value is 0, then the user password is stored in plain text.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

**Matching Rule**

booleanMatch

**Object ID**

2.16.840.1.113894.1.1.215

**Other**

Single-valued attribute.

## 8.2.382 orclPwDIlegalValues

### Description

Lists the common words and attribute types whose values cannot be used as a valid password. By default, all words are acceptable password values.

### Syntax

1.3.6.1.4.1.1466.115.121.1.15{1024} (Directory String, 1024 character maximum)

### Matching Rule

caseIgnoreMatch, caseIgnoreSubstringsMatch

### Object ID

2.16.840.1.113894.1.1.204

## 8.2.383 orclPwDIAccountLockedTime

### Description

The time when a user account was locked for a specific IP address.

### Syntax

1.3.6.1.4.1.1466.115.121.1.24 (Generalized Time)

### Matching Rule

generalizedTimeMatch

### Object ID

2.16.840.1.113894.1.1.211

### Other

Directory operational attribute.

Not user modifiable.

## 8.2.384 orclPwDIPFailureTime

### Description

The time of a password failure.

### Syntax

1.3.6.1.4.1.1466.115.121.1.24 (Generalized Time)

### Matching Rule

generalizedTimeMatch

### Object ID

2.16.840.1.113894.1.1.212

**Other**

Directory operational attribute.

Not user modifiable.

## 8.2.385 orclPwDIPLockout

**Description**

Whether to enable account lockouts for a specific IP address. The value can be 1 (for true) or 0 (for false).

**Syntax**

1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

**Matching Rule**

booleanMatch

**Object ID**

2.16.840.1.113894.1.1.200

**Other**

Single-valued attribute.

## 8.2.386 orclPwDIPLockoutDuration

**Description**

The number of seconds you want to enforce account lockout for a specific IP address. A user account stays locked even after the lockout duration has passed unless the user binds with the correct password.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.201

**Other**

Single-valued attribute.

## 8.2.387 orclPwDIPLMaxFailure

**Description**

The maximum number of failed logins from a specific IP address after which the account is locked.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.202

**Other**

Single-valued attribute.

**8.2.388 orclpwdmaxinactivitytime****Description**

Maximum period of time in seconds after which an inactive account is automatically locked.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.379

**Other**

Single-valued attribute.

**8.2.389 orclPwDMaxRptchars****Description**

Maximum number of times a single character type can be repeated in a password.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.415

**Other**

Single-valued attribute.

## 8.2.390 orclPwdMinAlphachars

### Description

Minimum number of alphabetic characters required in a password.

### Syntax

1.3.6.1.4.1.1466.115.121.1.27

### Matching Rule

integerMatch

### Object ID

2.16.840.1.113894.1.1.411

### Other

Single-valued attribute.

## 8.2.391 orclPwdMinSpecialchars

### Description

Minimum number of non-alphanumeric characters required in a password.

### Syntax

1.3.6.1.4.1.1466.115.121.1.27

### Matching Rule

integerMatch

### Object ID

2.16.840.1.113894.1.1.412

### Other

Single-valued attribute.

## 8.2.392 orclPwdMinUppercase

### Description

Minimum number of uppercase characters required in a password.

### Syntax

1.3.6.1.4.1.1466.115.121.1.27

### Matching Rule

integerMatch

### Object ID

2.16.840.1.113894.1.1.413

**Other**

Single-valued attribute.

**8.2.393 orclpwdminlowercase****Description**

orclpwdminlowercase

**Syntax**

Minimum number of lowercase characters required in a password.

1.3.6.1.4.1.1466.115.121.1.27

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.414

**Other**

Single-valued attribute.

**8.2.394 orclPwPolicyEnable****Description**

Whether to enable or disable the password policy. The value can be 1 (for enable) or 0 (for disable).

**Syntax**

1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

**Matching Rule**

booleanMatch

**Object ID**

2.16.840.1.113894.1.1.213

**Other**

Single-valued attribute.

**8.2.395 orclPwTrackLogin****Description**

Enables or disables tracking of user's last login time; 1 for enabling and 0 for disabling (default).

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.377

**Other**

Single-valued attribute

## 8.2.396 orclPwdVerifierParams

**Description**

This attribute contains the values of different password verifier types, such as:

orclpwdverifierparams;authpassword: crypto:SASL/MDS \$ realm:dc=com

orclpwdverifierparams;orclpasswordverifier: crypto:ORCLLM

orclpwdverifierparams;authpassword: crypto:ORCLWEBDAV \$ realm:dc=com

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15{256} (Directory String, 256 character maximum)

**Matching Rule**

caseIgnoreMatch, caseIgnoreSubstringsMatch

**Object ID**

2.16.840.1.113894.1.1.209

## 8.2.397 orclQueueDepth

**Description**

Indicates the queue depth.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.144

**Other**

Single-valued attribute.

## 8.2.398 orclQueueLatency

**Description**

Defines the queue latency.



**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.145

**Other**

Single-valued attribute.

**8.2.399 orclReadWaitThreads****Description**

Specifies the number of Oracle Internet Directory server threads waiting to read from the network.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.142

**Other**

Single-valued attribute.

**8.2.400 orclReqAttrCase****Description**

Disables or enables preserving the letter case of required attributes in search result. Allowed values are 0 (disable) or 1 (enable). The default value is 0.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.423

**Other**

Single-valued attribute

## 8.2.401 orclrefreshdgrmems

### Description

Refresh Dynamic Group Memberships.

### Syntax

1.3.6.1.4.1.1466.115.121.1.27

### Matching Rule

integerMatch (Integer)

### Object ID

2.16.840.1.113894.1.1.416

### Other

Single-valued attribute

## 8.2.402 orclReplAgreements

### Description

The DNs of the replication agreement entries.

### Syntax

1.3.6.1.4.1.1466.115.121.1.34 (Distinguished Name)

### Matching Rule

distinguishedNameMatch

### Object ID

2.16.840.1.113894.1.1.105

## 8.2.403 orclReplAttrConfl

### Description

Specifies whether timestamp or attribute version should be honored first during attribute level conflict resolution. 0 (default): timestamp first, 1: version number first

### Syntax

1.3.6.1.4.1.1466.115.121.1.27(Integer)

### Matching Rule

integerMatch

### Object ID

2.16.840.1.113894.1.1.899

### Other

Single valued attribute

## 8.2.404 orclreplautotune

### Description

Dynamically vary the number of threads assigned to transport and apply tasks based on load. 0: Off, 1: On.

If you set the server to auto tune, you must specify the number of maximum number of threads to be shared between these tasks. Restart server after changing.

### Syntax

Integer

### Matching Rule

integerMatch

### Object ID

2.16.840.1.113894.1.1.827

## 8.2.405 orclReplicaDN

### Description

For LDAP-based replication only. The DN of the consumer replica in the replication agreement.

### Syntax

1.3.6.1.4.1.1466.115.121.1.34 (Distinguished Name)

### Matching Rule

distinguishedNameMatch

### Object ID

2.16.840.1.113894.1.1.817

## 8.2.406 orclReplicaID

### Description

Naming attribute for the replica subentry. Its value is unique to each directory server node that is initialized at installation. The value of this attribute, assigned during installation, is unique to each directory node, and matches that of the `orclreplicaID` attribute at the root DSE. You cannot modify this value.

### Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

### Matching Rule

caseIgnoreMatch

### Object ID

2.16.840.1.113894.1.1.106

**Other**

Single-valued attribute.

## 8.2.407 orclReplicaSecondaryURI

**Description**

Contains the set of ldapURI formatted addresses that can be used if the orclReplicaURI values cannot be used.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.26 (IA5 String)

**Matching Rule**

caseExactIA5Match

**Object ID**

2.16.840.1.113894.1.1.815

## 8.2.408 orclReplicaState

**Description**

Defines the state of the replica. Possible values are:

- 0 (boot strapping)
- 1 (online)
- 2 (offline)
- 3 (bootstrap in progress)
- 4 (bootstrap in progress, cn=oraclecontext bootstrap has completed)
- 5 (bootstrap completed, failure detected for one or more naming contexts)
- 6 (database copy based add node)
- 7 (sync schema)
- 8 (boot strap without schema sync)

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.818

**Other**

Single-valued attribute.

## 8.2.409 orclreplicationid

**Description**

Unique identifier of a one-way, two-way, or peer-to-peer replication group

**Syntax**

Integer

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.509

## 8.2.410 orclReplicationProtocol

**Description**

Defines the replication protocol for change propagation to replica. Values are:

- ODS\_ASR\_1.0 (Oracle Database Advanced Replication-based protocol)
- ODS\_LDAP\_1.0 (LDAP-based replication)

You cannot modify this attribute.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch, caseIgnoreSubstringsMatch

**Object ID**

2.16.840.1.113894.1.1.29

**Other**

Single-valued attribute.

## 8.2.411 orclReplicationState

**Description**

Activation state of the replication server. 0-Inactive, 1-Active

**Syntax**

Integer

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.831

## 8.2.412 orclReplicaType

**Description**

Defines the type of replica such as read-only or read/write. Possible values are:

- 0 (Read/Write)
- 1 (Read-Only)

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.816

**Other**

Single-valued attribute.

## 8.2.413 orclReplicaURI

**Description**

Contains information in ldapURI format that can be used to open a connection to this replica.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.26 (IA5 String)

**Matching Rule**

caseExactIA5Match

**Object ID**

2.16.840.1.113894.1.1.814

**Other**

Single-valued attribute.

## 8.2.414 orclReplicaVersion

**Description**

Oracle Internet Directory version of the replica.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.820

**Other**

Single-valued attribute.

**8.2.415 orclreplmaxworkers****Description**

Maximum number of worker threads. Required if orclreplautotune is set.

**Syntax**

Integer

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.826

**8.2.416 orclreplusesasl;digest-md5****Description**

Use SASL for replication binds. Values are auth, auth-int, and auth-conf.

**Syntax**

Directory String

**Matching Rule**

caseIgnoreMatch; caseIgnoreSubstringMatch

**Object ID**

2.16.840.1.113894.1.1.829

**8.2.417 orclResourceIdentifier****Description**

Stores the resource identifier.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

**Matching Rule**

distinguishedNameMatch

**Object ID**

2.16.840.1.113894.1.1.348

## 8.2.418 orclResourceName

### Description

Specifies the name of the resource for which the connection information is being maintained.

### Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

### Matching Rule

caseIgnoreMatch, caseIgnoreSubstringsMatch

### Object ID

2.16.840.1.113894.1.1.350

## 8.2.419 orclResourceTypeName

### Description

Specifies the name of the resource, for example, database, XMLPDS, JDBCPS.

### Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

### Matching Rule

caseIgnoreMatch

### Object ID

2.16.840.1.113894.1.1.351

## 8.2.420 orclResourceViewers

### Description

Lists the users or groups of users who can view a Resource Access Descriptor.

### Syntax

1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

### Matching Rule

distinguishedNameMatch

### Object ID

2.16.840.1.113894.1.1.366



## 8.2.421 orclRevPwd

### Description

Reversible encrypted value of the user password. This attribute is generated only if the attribute value of [orclPwdEncryptionEnable](#) in the password policy entry is set to 1. This attribute cannot be queried.

### Syntax

1.3.6.1.4.1.1466.115.121.1.44{128} (Printable String, 128 character maximum)

### Matching Rule

octetStringMatch

### Object ID

2.16.840.1.113894.1.1.216

### Other

Directory operational attribute.

Not user modifiable.

## 8.2.422 orclrienabled

### Description

Enables referential integrity. 0: disabled, 1: enabled.

### Syntax

1.3.6.1.4.1.1466.115.121.1.27

### Matching Rule

integerMatch

### Object ID

2.16.840.1.113894.1.1.1300

### Other

Single-valued attribute

## 8.2.423 orclrscacheattr

### Description

Multi-valued attribute that specifies the Result Set Cache attributes. Default values are:

- dn: cn=dsaconfig,cn=configsets,cn=oracle internet directory
- orclrscacheattr: uid
- orclrscacheattr: mail
- orclrscacheattr: cn
- orclrscacheattr: orclguid

---

---

**Note:** Typically these attributes are not modified for the life of the entry. If an attribute has referential integrity enabled, that attribute should not be used.

---

---

**Syntax**

1.3.6.1.4.1.1466.115.121.1.44

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.624

**Other**

Multi-valued attribute.

## 8.2.424 orclTraceConnDN

**Description**

If `orclDebugFlag` is set to a value other than zero (0) and `orclTraceConnDN` specifies one or more connection DNs, Oracle Internet Directory server logs messages only for connections with specified DNs. Other messages are ignored.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.34 (Distinguished Name)

**Matching Rule**

distinguishedNameMatch

**Object ID**

2.16.840.1.113894.1.1.1051

**Other**

Multi-valued attribute.

## 8.2.425 orclTraceConnIP

**Description**

If `orclDebugFlag` is set to a value other than zero (0) and `orclTraceConnIP` specifies one or more connection IP addresses, Oracle Internet Directory server logs messages only for operations performed by the specified connection IP addresses. Other messages are ignored.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15{128} (Directory String, 128 character maximum)

**Matching Rule**

caseIgnoreMatch, caseIgnoreSubstringsMatch

**Object ID**

2.16.840.1.113894.1.1.1052

**Other**

Multi-valued attribute.

**8.2.426 orclSAMAccountName****Description**

Stores the value of Active Directory's `SAMAccountName` attribute. In Oracle Internet Directory, this attribute is defined as a directory string type. However, in Active Directory this attribute cannot accept any special or non-printable characters. If any entry is added in Oracle Internet Directory with this attribute, it can only contain a simple text string or synchronization from Oracle Internet Directory to Active Directory will fail.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.8.1.903

**Other**

Single-valued attribute.

**8.2.427 orclSASLAuthenticationMode****Description**

SASL authentication mode indicates different modes depending on the type of authentication required and the level of security, such as, `auth-only`, `auth-int`, or `auth-conf`.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.700

**Other**

Single-valued attribute.

## 8.2.428 orclSASLCipherChoice

**Description**

Contains the SASL cipher choice. when the authentication mode is auth-conf, the SASL cipher choices can be 3DES, DES, RC4, RC4-56, or RC4-40.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15{128} (Directory String, 128 character maximum)

**Matching Rule**

caseIgnoreMatch, caseIgnoreSubstringsMatch

**Object ID**

2.16.840.1.113894.1.1.702

## 8.2.429 orclSASLMechanism

**Description**

Indicates the different kinds of SASL mechanisms supported in the LDAP server. Currently, OID supports SASL-EXTERNAL and DIGEST-MD5.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15{128} (Directory String, 128 character maximum)

**Matching Rule**

caseIgnoreMatch, caseIgnoreSubstringsMatch

**Object ID**

2.16.840.1.113894.1.1.701

## 8.2.430 orclDumpFlag

**Description**

Determines whether to generate or stack file (default value 0) or OS level core file (value 1) in case the OID server crashes.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.407

**Other**

Single-valued attribute.

## 8.2.431 orclSearchBaseDN

### Description

Contains search base information to be used when performing the directory query for identity mapping.

### Syntax

1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

### Matching Rule

distinguishedNameMatch

### Object ID

2.16.840.1.113894.1.1.706

### Other

Single-valued attribute.

## 8.2.432 orclSearchFilter

### Description

Contains search filter information to be used when performing the directory query for identity mapping.

### Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

### Matching Rule

caseIgnoreMatch

### Object ID

2.16.840.1.113894.1.1.705

### Other

Single-valued attribute.

## 8.2.433 orclSearchScope

### Description

Contains search scope information to be used when performing the directory query for identity mapping.

### Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

### Matching Rule

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.707

**Other**

Single-valued attribute.

## 8.2.434 orclSecondaryUID

**Description**

Indicates the secondary UID of a user.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch, caseIgnoreSubstringsMatch

**Object ID**

2.16.840.1.113894.1.1.360

## 8.2.435 orclSequence

**Description**

Specifies the sequence number for audit log entries.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.62

## 8.2.436 orclServerAvgMemGrowth

**Description**

Specifies the Oracle Internet Directory server process memory growth as a percentage.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.148

**Other**

Single-valued attribute.

**8.2.437 orclServerMode****Description**

Specifies if data can be written to the server. Valid values are:

- r (read-only)
- rw (read/write)
- rm (read-modify, that is, to read and modify, but not to add or delete)

The default value is *rw*.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.51

**Other**

Single-valued attribute.

**8.2.438 orclServerProcs****Description**

Number of server processes to start. The default for *configset0* is 1. You cannot use a negative value for this attribute.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.364

**Other**

Single-valued attribute.

**8.2.439 orclServiceInstanceLocation****Description**

Specifies the DN of an instance of a service.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseExactMatch

**Object ID**

2.16.840.1.113894.1.1.1102

**Other**

Single-valued attribute.

## 8.2.440 orclServiceMember

**Description**

Identifies all the service instances that are members of a logical service entity.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

**Matching Rule**

distinguishedNameMatch

**Object ID**

2.16.840.1.113894.1.1.1005

## 8.2.441 orclServiceSubscriptionLocation

**Description**

Specifies the DN where the list of users subscribed to a service is available.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseExactMatch

**Object ID**

2.16.840.1.113894.1.1.1100

**Other**

Single-valued attribute

## 8.2.442 orclServiceSubType

**Description**

Identifies the sub-types of a Service e.g. IMAP, SMTP are sub-type of an e-mail service.



**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.1009

**Other**

Single-valued attribute

**8.2.443 orclServiceType****Description**

Identifies the type of Service e.g. Email, Calendar, and so forth.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.7.1.4

**Other**

Single-valued attribute

**8.2.444 orclSID****Description**

Stores the SID.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.7.1.5

**Other**

Single-valued attribute

## 8.2.445 orclsimplemodchglogattributes

**Description**

List of multivalued attributes that, when changed, cause a simplified change log to be generated.

**Syntax**

DN

**Matching Rule**

DistinguishedNameMatch

**Object ID**

2.16.840.1.113894.1.1.823

## 8.2.446 orclSizeLimit

**Description**

Maximum number of entries to be returned by a search.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.10

**Other**

Single-valued attribute

## 8.2.447 orclSkewedAttribute

**Description**

Attribute that contains names of attributes which are skewed. A skewed attribute has very different search response times depending on its value. You can uniform the response times for searches for such an attribute by adding it as a value of the orclskewedattribute attribute.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch, caseIgnoreSubstringsMatch

**Object ID**

2.16.840.1.113894.1.1.405

## 8.2.448 orclSkipRefInSQL

### Description

Specifies whether to skip referral in SQL generated for searches. Its default value is 0. Set it to 1 if there are no referral entries in the directory; this will help optimizing search performance.

### Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

### Matching Rule

integerMatch

### Object ID

2.16.840.1.113894.1.1.410

### Other

Single-valued attribute

## 8.2.449 orclSkipSpecialInFilter

### Description

Evaluates whether Oracle Internet Directory should skip the processing of special characters specified in filter values during a search operation. Its default value is 0.

0: Process the special characters specified in the filter value.

1: Do not process the special characters specified in the filter value.

### Syntax

1.3.6.1.4.1.1466.115.121.1.44

### Matching Rule

caseIgnoreMatch

### Object ID

2.16.840.1.113894.1.1.629

### Other

Single-valued attribute

## 8.2.450 orclSMSpec

### Description

Represents a structural object class that includes common attributes for server manageability object classes.

### Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch, caseIgnoreSubstringsMatch

**Object ID**

2.16.840.1.113894.1.1.185

## 8.2.451 orclSQLexFetchLatency

**Description**

Reserved for future use.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.132

**Other**

Single-valued attribute

## 8.2.452 orclSQLGenReusedParsed

**Description**

Reserved for future use.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.134

**Other**

Single-valued attribute

## 8.2.453 orclSSLAuthentication

**Description**

Type of SSL authentication to use for this instance of Oracle Internet Directory server. The default value of 1, specifies no SSL authentication. Different instances can have different values. One-way and two-way SSL authentication requires a wallet. You may use one of the following three values:

- 1 = Neither the client nor the server authenticates itself to the other. No certificates are sent or exchanged. If you selected the SSL Enabled check box on the Credentials tab, and choose this option, then only SSL encryption/decryption is used.
- 32 = One-way authentication. Only the directory server authenticates itself to the client by sending its certificate to the client.
- 64 = Two-way authentication. Both client and server send certificates to each other.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.13

**Other**

Single-valued attribute

## 8.2.454 orclSSLCipherSuite

**Description**

A cipher suite is 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. The following cipher suites are supported:

**Table 8–3 SSL Cipher Suites Supported in Oracle Internet Directory**

Cipher Suite	Authentication	Encryption	Data Integrity
SSL_RSA_WITH_3DES_EDE_CBC_SHA	RSA	3DES	SHA
SSL_RSA_WITH_RC4_128_SHA	RSA	RC4	SHA
SSL_RSA_WITH_RC4_128_MD5	RSA	RC4	MD5
SSL_RSA_WITH_DES_CBC_SHA	RSA	DES	SHA
SSL_RSA_EXPORT_WITH_RC4_40_MD5	RSA	RC4_40	MD5
SSL_RSA_EXPORT_WITH_DES40_CBC_SHA	RSA	DES40	SHA
SSL_DH_anon_WITH_3DES_EDE_CBC_SHA	None	3DES	SHA
SSL_DH_anon_WITH_RC4_128_MD5	None	RC4	MD5
SSL_DH_anon_WITH_DES_CBC_SHA	None	DES	SHA
SSL_RSA_WITH_AES_128_CBC_SHA	RSA	AES	SHA
SSL_RSA_WITH_AES_256_CBC_SHA	RSA	AES	SHA

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15{128} (Directory String, 128 character maximum.)

**Matching Rule**

caseIgnoreMatch, caseIgnoreSubstringsMatch

**Object ID**

2.16.840.1.113894.1.1.19

**8.2.455 orclSSLEnable****Description**

Flag for enabling or disabling SSL. Use this flag when you use different instances of the same server for either SSL or non-SSL. Allowed values are:

- 0—for non-secure operation only
- 1—for SSL authentication only
- 2—for both non-secure operation and SSL authentication

The default value is 2.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.14

**Other**

Single-valued attribute

**8.2.456 orclsslinteropmode****Description**

Enable SSL interoperability with Oracle legacy applications using no-auth mode.

Starting with Oracle Internet Directory 11g Release 1 (11.1.1.7.0), the default value is disabled (orclsslinteropmode = 0), in order to be fully compliant with the JDK SSL.

In no-auth mode, Oracle legacy components developed before 11g Release 1 (11.1.1) such as legacy LDAP C clients can connect with Oracle Internet Directory only by using an instance that has interoperability mode enabled (orclsslinteropmode = 1).

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.422

**Other**

Single-valued attribute

**8.2.457 orclSSLPort****Description**

The default SSL default port for the directory server. Default value is 3133. When you run the directory in the secure mode, it listens at default port 3133 and accepts only SSL-based TCP/IP connections. (When you run the directory in the normal mode, it listens at default port 389, accepting normal TCP/IP connections.) You might want to change this port when you add multiple LDAP server instances.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.17

**Other**

Single-valued attribute

**8.2.458 orclSSLVersion****Description**

SSL version. The default value is 3.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.18

**Other**

Single-valued attribute

**8.2.459 orclSSLWalletURL****Description**

Sets the location of the Oracle Wallet. You initially set this value when you create the wallet. If you elect to change the location of the Oracle Wallet, you must change this parameter. You must set the wallet location on both the client and the server. For example, on UNIX, you could set this parameter as follows:

```
file:/home/my_dir/my_wallet
```

On Microsoft Windows, you could set this parameter as follows:

```
file:C:\my_dir\my_wallet
```

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15{128} (Directory String, 128 character maximum)

**Matching Rule**

caseIgnoreMatch, caseIgnoreSubstringsMatch

**Object ID**

2.16.840.1.113894.1.1.15

**Other**

Single-valued attribute

## 8.2.460 orclStatsDN

**Description**

Specifies list of user DN's for which to track LDAP operations.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

**Matching Rule**

distinguishedNameMatch

**Object ID**

2.16.840.1.113894.1.1.187

## 8.2.461 orclStatsFlag

**Description**

Enable or disable the Oracle Internet Directory Server Manageability framework. To enable, set this to 1. To disable, set it to 0.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.197

**Other**

Single-valued attribute.



## 8.2.462 orclStatsLevel

### Description

Level of statistics collection for users. There is only one valid value in this release, 1. Specifying this value collects the number of bind and compare operations against the directory and the user who performed each one.

### Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

### Matching Rule

integerMatch

### Object ID

2.16.840.1.113894.1.1.199

### Other

Single-valued attribute.

## 8.2.463 orclStatsOp

### Description

Reserved for future use.

### Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

### Matching Rule

integerMatch

### Object ID

2.16.840.1.113894.1.1.188

### Other

Single-valued attribute.

## 8.2.464 orclStatsPeriodicity

### Description

Time interval in minutes for gathering server manageability statistics. The default value is 60.

### Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

### Matching Rule

integerMatch

**Object ID**

2.16.840.1.113894.1.1.198

**Other**

Single-valued attribute.

## 8.2.465 orclStatus

**Description**

Depending on the context of the object that it is applied to, like a service, it indicates if the service is available or not.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch, caseIgnoreSubstringsMatch

**Object ID**

2.16.840.1.113894.9.1.9

## 8.2.466 orclSUAccountLocked

**Description**

Determines whether a superuser account is locked.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.192

**Other**

Single-valued attribute.

Directory operational attribute.

Not user modifiable.

## 8.2.467 orclSubscriberDisable

**Description**

Reserved for future use.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.100

**Other**

Single-valued attribute.

**8.2.468 orclSubscriberFullName****Description**

Stores the full name of the configured realm.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.333

**Other**

Single-valued attribute.

**8.2.469 orclSubscriberNickNameAttribute****Description**

Stores a name of an attribute that holds the unique identifier of a realm.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.302

**Other**

Single-valued attribute.

**8.2.470 orclSubscriberSearchBase****Description**

Specifies the DIT node that contains all realms.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

**Matching Rule**

distinguishedNameMatch

**Object ID**

2.16.840.1.113894.1.1.301

## 8.2.471 orclSubscriberType

**Description**

Defines the type of realm created.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.331

**Other**

Single-valued attribute.

## 8.2.472 orclSuffix

**Description**

To have the directory server manage part of an LDAP directory, you can specify the highest level parent DNs in the server configuration. These DNs are called suffixes. The server can access all objects in the directory that are below the specified suffix in the directory hierarchy. This attribute is part of the root DSE (DSA-Specific Entry). The root DSE contains a number of attributes that store information about the directory server itself.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15{128} (Directory String, 128 character maximum)

**Matching Rule**

caseIgnoreMatch, caseIgnoreSubstringsMatch

**Object ID**

2.16.840.1.113894.1.1.6

**Other**

Single-valued attribute.

## 8.2.473 orclSuiteType

**Description**

Identifies the type of suite e.g ocs, ebiz, and so forth.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.1011

**Other**

Single-valued attribute.

## 8.2.474 orclSULoginFailureCount

**Description**

The number of failed login attempts for the directory superuser.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.191

**Other**

Single-valued attribute.

Directory operational attribute.

Not user modifiable.

## 8.2.475 orclSUName

**Description**

The distinguished name of the directory superuser account, for example, cn=orcladmin.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.12

**Matching Rule**

distinguishedNameMatch

**Object ID**

2.16.840.1.113894.1.1.8

**Other**

Single-valued attribute.

## 8.2.476 orclSUPassword

**Description**

Oracle Internet Directory superuser password.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15{128} (Directory String, 128 character maximum)

**Matching Rule**

caseIgnoreMatch, caseIgnoreSubstringsMatch

**Object ID**

2.16.840.1.113894.1.1.9

**Other**

Single-valued attribute.

## 8.2.477 orclSystemName

**Description**

Identifies the host name on which a particular instance of a service is running.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.7.1.3

**Other**

Single-valued attribute.

## 8.2.478 orclTcpConnToClose

**Description**

Specifies the number of clients for which the Oracle Internet Directory server will close TCP connections.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.153

**Other**

Single-valued attribute.

**8.2.479 orclTcpConnToShutDown****Description**

Specifies the number of clients for which the Oracle Internet Directory server will shut down TCP connections.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.152

**Other**

Single-valued attribute.

**8.2.480 orclThreadSpawnFailed****Description**

Reserved for future use.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.154

**Other**

Single-valued attribute.

**8.2.481 orclThreadsPerSupplier****Description**

Specifies the number of threads per supplier for the Oracle directory replication server.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integermatch

**Object ID**

2.16.840.1.113894.1.1.31

**Other**

DSA operational attribute.

## 8.2.482 orclTimeLimit

**Description**

Maximum number of seconds allowed for a search to be completed. The default value is 3600.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.65

**Other**

Single-valued attribute.

## 8.2.483 orclTimeZone

**Description**

Specifies the time zone applicable for a user location.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.311

## 8.2.484 orclLimitMode

**Description**

Defines the time limit mode.



**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.406

**Other**

Single-valued attribute.

**8.2.485 orclTotFreePhyMem****Description**

Stores the total amount of free system physical memory.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.146

**Other**

Single-valued attribute.

**8.2.486 orclTraceDimesionLevel****Description**

Reserved for future use.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.174

**Other**

Single-valued attribute.

## 8.2.487 orclTraceFileLocation

### Description

Reserved for future use.

### Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

### Matching Rule

caseIgnoreMatch, caseIgnoreSubstringsMatch

### Object ID

2.16.840.1.113894.1.1.176

### Other

Single-valued attribute.

## 8.2.488 orclTraceFileSize

### Description

Reserved for future use.

### Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

### Matching Rule

integerMatch

### Object ID

2.16.840.1.113894.1.1.177

### Other

Single-valued attribute.

## 8.2.489 orclTraceLevel

### Description

Reserved for future use.

### Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

### Matching Rule

integerMatch

### Object ID

2.16.840.1.113894.1.1.173

**Other**

Single-valued attribute.

**8.2.490 orclTraceMode****Description**

Reserved for future use.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch, caseIgnoreSubstringsMatch

**Object ID**

2.16.840.1.113894.1.1.175

**Other**

Single-valued attribute.

**8.2.491 orclTrustedApplicationGroup****Description**

Identifies the DN of the group that list all the applications that specific application trusts for Service to Service Authentication.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

**Matching Rule**

distinguishedNameMatch

**Object ID**

2.16.840.1.113894.1.1.368

**8.2.492 orclTraceMode****Description**

Reserved for future use.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch, caseIgnoreSubstringsMatch

**Object ID**

2.16.840.1.113894.1.1.175

**Other**

Single-valued attribute.

## 8.2.493 orclTxnMaxOperations

**Description**

Maximum number of operations allowed in a transaction.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.381

**Other**

Single-valued attribute

## 8.2.494 orclTxnTimeLimit

**Description**

Maximum allowed time in a transaction (sec).

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.380

**Other**

Single-valued attribute

## 8.2.495 orclUIAccessibilityMode

**Description**

Set to TRUE to display a user interface that is accessible to people with impaired vision.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

**Matching Rule**

booleanMatch

**Object ID**

2.16.840.1.113894.1.1.367

**Other**

Single-valued attribute.

**8.2.496 orclUniqueAttrName****Description**

The name of an attribute that you want to be unique. Autoboost uniqueness means that each entry must have a unique value for this attribute type.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.500

**Other**

Single-valued attribute.

**8.2.497 orclUniqueEnable****Description**

Disables or enables attribute uniqueness constraints. Allowed values are 0 (disable) or 1 (enable). The default value is 0.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.508

**Other**

Single-valued attribute.

**8.2.498 orclUniqueObjectClass****Description**

Specifies an object class filter for an attribute uniqueness constraint entry. This means the attribute specified in `orclUniqueAttrName` must be unique in an instance of this object class.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.503

**Other**

Single-valued attribute.

**8.2.499 orclUniqueScope****Description**

The scope of the attribute uniqueness constrain in the DIT. Allowed values are:

- `base`—Searches the root entry only
- `onelevel`—Searches one level only
- `sub`—Searches the entire directory

The default value is `sub`.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.501

**Other**

Single-valued attribute.

**8.2.500 orclUniqueSubtree****Description**

When multiple attribute uniqueness constraints have the same values in `orclUniqueAttrName`, `orclUniqueScope` and `orclUniqueObjectClass`, but different values in `orclUniquesubtree`, the union of subtree scopes specified by those attribute uniqueness constraints is checked.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

**Object ID**

2.16.840.1.113894.1.1.502

**Other**

Single-valued attribute.

**8.2.501 orclUnsyncRevPwd****Description**

This attribute stores a password that is not synchronized with the entry in the userpassword.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.44{128} (Printable String, 128 character maximum)

**Matching Rule**

octetStringMatch

**Object ID**

2.16.840.1.113894.1.1.217

**Other**

Directory operational attribute.

Not user modifiable.

**8.2.502 orclUpdateSchedule****Description**

Replication update interval for new changes and those being retried. The value is in seconds.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27

**Matching Rule**

integermatch

**Object ID**

2.16.840.1.113894.1.1.30

**Other**

Directory operational attribute.

Not user modifiable.

Single-valued attribute.

## 8.2.503 orclUpgradelnProgress

### Description

Indicates whether rolling upgrade is in progress.

### Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

### Matching Rule

caseIgnoreMatch

### Object ID

2.16.840.1.113894.1.1.104

### Other

Single-valued attribute.

## 8.2.504 orclUserDN

### Description

The distinguished name (DN) of the user who performed an operation.

### Syntax

1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

### Matching Rule

distinguishedNameMatch

### Object ID

2.16.840.1.113894.1.1.61

## 8.2.505 orclUserIDAttribute

### Description

Specifies the attribute to use as the user identifier value when accessing the resource.

### Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

### Matching Rule

caseIgnoreMatch, caseIgnoreSubstringsMatch

### Object ID

2.16.840.1.113894.1.1.352

### Other

Single-valued attribute.



## 8.2.506 orclUserModifiable

### Description

Specifies if the data is modifiable by the user that this resource access descriptor entry is created for.

### Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

### Matching Rule

caseIgnoreMatch, caseIgnoreSubstringsMatch

### Object ID

1.2.3.4.5.6.1.11

## 8.2.507 orclUserObjectClasses

### Description

A list of the object classes that comprise a user entity.

### Syntax

1.3.6.1.4.1.1466.115.121.1.15

### Matching Rule

caseIgnoreMatch

### Object ID

2.16.840.1.113894.1.1.329

## 8.2.508 orclUserPrincipalName

### Description

This is the Kerberos user principal name for Microsoft Active Directory users.

### Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

### Matching Rule

caseIgnoreMatch

### Object ID

2.16.840.1.113894.8.1.904

### Other

Single-valued attribute.

## 8.2.509 orclVersion

### Description

The release version of the Oracle Internet Directory server.

### Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

### Matching Rule

caseIgnoreMatch

### Object ID

2.16.840.1.113894.7.1.1

### Other

Single-valued attribute.

## 8.2.510 orclWirelessAccountNumber

### Description

Stores the wireless account number of a user.

### Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

### Matching Rule

caseIgnoreMatch

### Object ID

2.16.840.1.113894.1.1.365

### Other

Single-valued attribute.

## 8.2.511 orclWorkflowNotificationPref

### Description

Identifies workflow notification preferences for a user.

### Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

### Matching Rule

caseIgnoreMatch

### Object ID

2.16.840.1.113894.1.1.313

## 8.2.512 orclWriteWaitThreads

**Description**

Specifies the number of Oracle Internet Directory server threads waiting to write to the network.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.143

**Other**

Single-valued attribute.

## 8.2.513 owner

**Description**

Specifies the distinguished name (DN) of some object which has some responsibility for the associated object.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

**Matching Rule**

distinguishedNameMatch

**Object ID**

2.5.4.32

## 8.2.514 pilotStartTime

**Description**

The time stamp of when pilot mode was started for a replica.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.24 (Generalized Time)

**Matching Rule**

generalizedTimeMatch

**Object ID**

2.16.840.1.113894.1.1.825

**Other**

Single-valued attribute.

Directory operational attribute.

Not user modifiable.

## 8.2.515 preferredServerList

### Description

The IP addresses of the preferred servers that a directory user agent should use in a space separated list. The servers in this list are tried in order before those in the [defaultServerList](#) until a successful connection is made. This has no default value. At least one server must be specified in either preferredServerList or defaultServerList.

### Syntax

1.3.6.1.4.1.1466.115.121.1.26 (Printable String)

### Matching Rule

caseIgnoreIA5Match

### Object ID

1.3.6.1.4.1.11.1.3.1.1.2

### Other

Single-valued attribute.

## 8.2.516 profileTTL

### Description

The time to live before a client directory user agent (DUA) should re-read this configuration profile. The values for profileTTL can be zero, to indicate no expiration, or a positive integer combined with one of the following letters to indicate the unit of measure:

d: indicates days

h: indicates hours

m: indicates minutes

s: indicates seconds

### Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

### Matching Rule

integerMatch

### Object ID

1.3.6.1.4.1.11.1.3.1.1.7

### Other

Single-valued attribute.

## 8.2.517 protocolInformation

**Description**

This attribute is used in conjunction with the `presentationAddress` attribute, to provide additional information to the Open System Interconnection (OSI) network service.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.42 (Protocol Information)

**Matching Rule**

`protocolInformationMatch`

**Object ID**

2.5.4.48

## 8.2.518 pwdAccountLockedTime

**Description**

The time stamp of when a user's account was locked.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.24 (Generalized Time)

**Matching Rule**

`generalizedTimeMatch`

**Object ID**

1.3.6.1.4.1.42.2.27.8.1.17

**Other**

Single-valued attribute.

Directory operational attribute.

No user modification.

## 8.2.519 pwdAllowUserChange

**Description**

Reserved for future use.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

**Matching Rule**

`booleanMatch`

**Object ID**

1.3.6.1.4.1.42.2.27.8.1.14

**Other**

Single-valued attribute.

## 8.2.520 pwdChangedTime

**Description**

The time stamp indicating when the user's current password was created or modified.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.24 (Generalized Time)

**Matching Rule**

generalizedTimeMatch

**Object ID**

1.3.6.1.4.1.42.2.27.8.1.16

**Other**

Single-valued attribute.

Directory operational attribute.

No user modification.

## 8.2.521 pwdCheckSyntax

**Description**

A value of 1 (default) means passwords are checked for syntax errors. A value of 0 means syntax checking is disabled.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

1.3.6.1.4.1.42.2.27.8.1.5

**Other**

Single-valued attribute.

## 8.2.522 pwdExpirationWarned

**Description**

The time stamp when the first password expiration warning was sent to the user.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.24 (Generalized Time)

**Matching Rule**

generalizedTimeMatch

**Object ID**

1.3.6.1.4.1.42.2.27.8.1.18

**Other**

Directory operational attribute.

No user modification.

**8.2.523 pwdExpireWarning****Description**

The number of seconds before a password expires that a warning should be sent to the user. The user will see the warning when they attempt to log on during the warning period. If the user does not modify the password before it expires, the user is locked out until the password is changed by the administrator. The default value is 0, which means no warnings are sent.

For this feature to work, the client application must support it.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

1.3.6.1.4.1.42.2.27.8.1.7

**Other**

Single-valued attribute.

**8.2.524 pwdFailureCountInterval****Description**

The number of seconds after which the password failure times are purged from the user entry. If this attribute is not present, or if it has a value of 0, then failure times are never purged. The default value is 0.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

1.3.6.1.4.1.42.2.27.8.1.12

**Other**

Single-valued attribute.

## 8.2.525 pwdFailureTime

**Description**

The time stamp of consecutive failed login attempts by the user.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.24 (Generalized Time)

**Matching Rule**

generalizedTimeMatch

**Object ID**

1.3.6.1.4.1.42.2.27.8.1.19

**Other**

Directory operational attribute.

No user modification.

## 8.2.526 pwdGraceLoginLimit

**Description**

Maximum number of grace logins allowed after a password expires. The default value is 0 (no grace logins allowed). The recommended value is 3.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

1.3.6.1.4.1.42.2.27.8.1.8

**Other**

Single-valued attribute.

## 8.2.527 pwdGraceLoginTimeLimit

**Description**

Number of seconds after account lockout to allow grace logins.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27(Integer)



**Matching Rule**

integerMatch

**Object ID**

2.16.840.1.113894.1.1.418

**Other**

Single-valued attribute.

**8.2.528 pwdGraceUseTime****Description**

The time stamps of each grace login for a user.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.24 (Generalized Time)

**Matching Rule**

generalizedTimeMatch

**Object ID**

1.3.6.1.4.1.42.2.27.8.1.21

**Other**

Directory operational attribute.

No user modification.

**8.2.529 pwdHistory****Description**A history of a user's previous passwords. The number of passwords stored in the history is determined by the [pwdInHistory](#) attribute.**Syntax**

1.3.6.1.4.1.1466.115.121.1.44{128} (Printable String, 128 character maximum)

**Matching Rule**

octetStringMatch

**Object ID**

1.3.6.1.4.1.42.2.27.8.1.20

**Other**

Single-valued attribute.

Directory operational attribute.

No user modification.

## 8.2.530 pwdInHistory

### Description

Number of previous passwords to be stored in the password history ([pwdHistory](#)). If a user attempts to reuse one of the passwords stored in the history, then the password is rejected. The default value is 0 (no previous passwords stored in the history).

### Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

### Matching Rule

integerMatch

### Object ID

1.3.6.1.4.1.42.2.27.8.1.4

### Other

Single-valued attribute.

## 8.2.531 pwdLockout

### Description

Specification for whether users are locked out of the directory after the number of consecutive failed bind attempts specified by [pwdMaxFailure](#). If the value of this policy attribute is TRUE, then users are locked out. If this attribute is not present, or if the value is FALSE, then users are not locked out and the value of [pwdMaxFailure](#) is ignored. By default, account lockout is enforced.

### Syntax

1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

### Matching Rule

booleanMatch

### Object ID

1.3.6.1.4.1.42.2.27.8.1.9

### Other

Single-valued attribute.

## 8.2.532 pwdLockoutDuration

### Description

The number of seconds a user is locked out of the directory if both of the following are true:

- Account lockout is enabled.
- The user has been unable to bind successfully to the directory for at least the number of times specified by [pwdMaxFailure](#).

You can set user lockout for a specific duration, or until the administrator resets the user's password. A default value of 0 (zero) means that the user is locked out forever. A user account stays locked even after the lockout duration has passed unless the user binds with the correct password.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

1.3.6.1.4.1.42.2.27.8.1.10

**Other**

Single-valued attribute.

### 8.2.533 pwdMaxAge

**Description**

The maximum number of seconds that a given password is valid. If this attribute is not present, or if the value is 0 (zero), then the password does not expire. By default, the passwords expire in 60 days.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

1.3.6.1.4.1.42.2.27.8.1.3

**Other**

Single-valued attribute.

### 8.2.534 pwdMaxFailure

**Description**

The number of consecutive failed bind attempts after which a user account is locked. If this attribute is not present, or if the value is 0 (zero), then the account is not locked due to failed bind attempts, and the value of the password lockout policy is ignored. The default is 4.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

1.3.6.1.4.1.42.2.27.8.1.11

**Other**

Single-valued attribute.

## 8.2.535 pwdMinAge

**Description**

This attribute holds the number of seconds that must elapse between modifications to the password. If this attribute is not present, 0 seconds is assumed.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

1.3.6.1.4.1.42.2.27.8.1.2

**Other**

Single-valued attribute.

## 8.2.536 pwdMinLength

**Description**

The minimum number of characters required in a password. The default is 5. The value for this attribute must be at least 1.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

**Matching Rule**

integerMatch

**Object ID**

1.3.6.1.4.1.42.2.27.8.1.6

**Other**

Single-valued attribute.

## 8.2.537 pwdMustChange

**Description**

Indicator of whether users must change their passwords after the first login, or after the password is reset by the administrator. Enabling this option requires users to change their passwords even if user-defined passwords are disabled. By default, users need not change their passwords after reset. Allowed values are 1 (true) or 0 (false).

**Syntax**

1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

**Matching Rule**

booleanMatch

**Object ID**

1.3.6.1.4.1.42.2.27.8.1.13

**Other**

Single-valued attribute.

**8.2.538 pwdpolicysubentry****Description**

DN of the password policy applicable at the subtree rooted at this DN.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.34

**Matching Rule**

distinguishedNameMatch

**Object ID**

2.16.840.1.113894.1.1.417

**8.2.539 pwdReset****Description**

Indicator that the password has been reset and must be changed by the user on first authentication. Allowed values are TRUE or FALSE.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

**Matching Rule**

booleanMatch

**Object ID**

1.3.6.1.4.1.42.2.27.8.1.22

**Other**

Single-valued attribute.

Directory operational attribute.

Not user modifiable.

## 8.2.540 pwdSafeModify

**Description**

Indicator of whether user must supply old password with new one when modifying password. By default, the old password is not required. Allowed values are TRUE or FALSE.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

**Matching Rule**

booleanMatch

**Object ID**

1.3.6.1.4.1.42.2.27.8.1.15

**Other**

Single-valued attribute.

## 8.2.541 ref

**Description**

A named reference. Values placed in the attribute must conform to the specification given for the [labeledURI](#) attribute (RFC 2079).

**Syntax**

1.3.6.1.4.1.1466.115.121.1.26 (IA5 String)

**Matching Rule**

caseExactIA5Match

**Object ID**

2.16.840.1.113730.3.1.34

**Other**

DSA operational attribute.

## 8.2.542 seeAlso

**Description**

Specifies the distinguished names of other directory objects which may be other aspects (in some sense) of the same real world object.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

**Matching Rule**

distinguishedNameMatch

**Object ID**

2.5.4.34

**8.2.543 serverName****Description**

The name of the server involved in an Oracle Directory Integration and Provisioning change subscription.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

caseIgnoreMatch

caseignoresubstringsmatch

**Object ID**

2.16.840.1.113894.1.1.34

**8.2.544 serviceAuthenticationMethod****Description**

The authentication method for the service.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

**Matching Rule**

N/A

**Object ID**

1.3.6.1.4.1.11.1.3.1.1.15

**8.2.545 serviceCredentialLevel****Description**

The credential level to be used by a service. The default value for all services is NULL. The supported credential levels are `anonymous` or `proxy`.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.26 (IA5 String)

**Matching Rule**

N/A

**Object ID**

1.3.6.1.4.1.11.1.3.1.1.13

## 8.2.546 serviceSearchDescriptor

### Description

Defines how and where an LDAP naming service client should search for information for a particular service. Contains a service name, followed by one or more semicolon-separated base-scope-filters.

### Syntax

1.3.6.1.4.1.1466.115.121.1.26 (IA5 String)

### Matching Rule

caseExactIA5Match

### Object ID

1.3.6.1.4.1.11.1.3.1.1.8

## 8.2.547 sn

### Description

The surname or last name of a user.

### Syntax

1.3.6.1.4.1.1466.115.121.1.15{32768} (Directory String, 32768 character maximum)

### Matching Rule

caseIgnoreMatch, caseIgnoreSubstringsMatch

### Object ID

2.5.4.4

## 8.2.548 supportedcontrol

### Description

List of controls supported by directory server.

### Syntax

OID

### Object ID

1.3.6.1.4.1.1466.101.120.13

## 8.2.549 supportedextension

### Description

List of extended operation supported

### Syntax

OID



**Object ID**

1.3.6.1.4.1.1466.101.120.7

**8.2.550 supportedldapversion****Description**

LDAP versions supported.

**Syntax**

Integer

**Object ID**

1.3.6.1.4.1.1466.101.120.15

**8.2.551 uniqueMember****Description**

The distinguished name for the member of a group.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.34 (Distinguished Name)

**Matching Rule**

distinguishedNameMatch

**Object ID**

2.5.4.50

**8.2.552 supportedsaslmmechanisms****Description**

List of SASL mechanism supported.

**Syntax**

Directory String

**Matching Rule****Object ID**

1.3.6.1.4.1.1466.101.120.14

**8.2.553 userCertificate;binary****Description**

The user's certificate.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.8 (Certificate)

**Matching Rule**

octetStringMatch

**Object ID**

2.5.4.36

## 8.2.554 userPassword

**Description**

The password used to authenticate a user to the directory.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.44{128} (Printable String, 128 character maximum)

**Matching Rule**

octetStringMatch

**Object ID**

2.5.4.35

**Other**

Single-valued attribute.

## 8.2.555 userPKCS12

**Description**

PKCS#12 PFX PDU for exchange of personal identity information.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.5 (Binary)

**Matching Rule**

N/A

**Object ID**

2.16.840.1.113730.3.1.216

## 8.2.556 x509issuer

**Description**

The DN of the certificate authority who issued the X.509 certificate revocation list.

**Syntax**

1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

**Matching Rule**

distinguishedNameMatch

**Object ID**

1.3.6.1.4.1.10126.1.5.3.4



# Part III

---

## Appendixes

This part contains the following appendix:

- [Appendix A, "LDIF File Format"](#)



---

---

# LDIF File Format

This appendix provides information about creating LDAP Data Interchange Files (LDIF) that can be used by the Oracle Internet Directory command-line tools.

This appendix includes the following sections:

- Section A.1, "General LDIF Formatting Rules"
- Section A.2, "LDIF Format for Entries"
- Section A.3, "LDIF Format for Adding Schema Elements"

## A.1 General LDIF Formatting Rules

LDIF formats are defined by the Internet Engineering Task Force (IETF) in RFC 2849. Visit the IETF Web site at <http://www.ietf.org/rfc/rfc2849.txt> for more information about LDIF formatting rules. This section explains some general rules for formatting LDIF files.

### A.1.1 Line Types and White Space

Each line in an LDIF file must be correctly formatted in order to be read by the Oracle Internet Directory command-line tools. White space and line breaks must be used carefully.

Each line in an LDIF file is terminated with a line feed, which is <LF> on UNIX or <CR><LF> on Windows. In LDIF you can have the following types of lines:

- **Directive Line** - Any line that does not begin with either a SPACE or # (hash). A directive line specifies either some type of data in an entry or an operation to perform.
- **Continuation Line** - A line that begins with a SPACE denotes that the characters following the space are part of the previous line.
- **Blank Line** - Blank lines are used to separate entries and are typically created with the ENTER key.
- **Comment Line** - A comment line begins with a # (hash). Comments are ignored by the Oracle Internet Directory command-line tools.
- **Separator Line** - A line that starts with a - (dash) character is used to end an operation. It denotes that the next line begins a new operation directive.

Unnecessary space characters in the LDIF input file, such as a space at the end of an attribute value, will cause the LDAP operations to fail.

## A.1.2 Sequencing of Entries

The sequence of entries in your LDIF file must follow the Directory Information Tree (DIT) from the top down. Parent entries should be listed before their children entries. Any attributes or object classes used in an entry must exist in the schema or be added to the schema before they can be used. Separate entries with a blank line.

## A.1.3 Binary Files

Reference binary files, such as photographs, with the absolute address of the file preceded by a / (forward slash).

## A.1.4 Non-Printing Characters in Attribute Values

Non-printing characters and tabs are represented in attribute values as base-64 encoding.

## A.2 LDIF Format for Entries

The standard format for directory entries is as follows:

```
dn: distinguished_name
changetype: add|delete|modify|modrdn|moddn
attribute_type: attribute_value
...
objectClass: object_class_value
...
```

### The dn Directive

The `dn` directive defines the distinguished name (DN) of an entry. It is assumed that all lines below a `dn` directive belong to that entry until you add a space in the LDIF file to denote a separate entry. The following example shows a `dn` directive line:

```
dn: cn=Mary Jones,ou=Sales,dc=company,dc=com
```

### The changetype Directive

The `changetype` directive defines the operation you want to perform on the entry. The operations that you specify with the `changetype` directive are:

- `add` - See [Section A.2.1, "LDIF Format for Adding Entries"](#) for syntax and examples.
- `delete` - See [Section A.2.2, "LDIF Format for Deleting Entries"](#) for syntax and examples.
- `modify` - [Section A.2.3, "LDIF Format for Modifying Entries"](#) for syntax and examples.
- `modrdn` - See [Section A.2.4, "LDIF Format for Modifying the RDN of an Entry"](#) for syntax and examples.
- `moddn` - See [Section A.2.5, "LDIF Format for Modifying the DN of an Entry"](#) for syntax and examples.

If `changetype` directive is omitted, then an `add` operation is assumed if using `bulkload`, `ldapadd` or `ldapaddmt`. A `delete` operation is assumed if using `bulkdelete` or `ldapdelete`. All other operations must specify a `changetype: directive`.



### The *attribute\_type* Directive

The *attribute\_type* directive is used to specify an attribute type name and value pair. The entry will have an *attribute\_type* directive for each attribute in the entry. For example, here is an *attribute\_type* directive for the attribute type named *cn* where the value is *Mary Smith*.

```
cn: Mary Smith
```

### The *objectClass* Directive

The *objectClass* directive is used to specify the object class that is associated with the entry. If an entry uses multiple object classes, then it will have an *objectClass* directive for each object class used. For example, here are the object classes used to define a user entry.

```
objectClass: orclUserV2
objectClass: organizationalPerson
objectClass: person
objectClass: top
```

Note that if an object class has required attributes, you must supply a value for those attributes using *attribute\_type* directives.

## A.2.1 LDIF Format for Adding Entries

The following example shows a file entry for an employee. The first line contains the DN. The second line contains the *changetype: add* directive. The lines that follow begin with the name for an attribute type, followed by the value to be associated with that attribute. Note that the *photo* attribute value begins with a forward slash (*\*) to denote that it is a binary file reference. Use an empty line at the end of the entry as a separator.

```
dn: cn=Suzie Smith,ou=Server Technology,o=Acme, c=US
changetype: add
cn: Suzie Smith
cn: Suzie
sn: Smith
mail: ssmith@us.Acme.com
telephoneNumber: 69332
photo: \${ORACLE_INSTANCE}/empdir/photog/ssmith.jpg
objectClass: organizationalPerson
objectClass: person
objectClass: top
```

## A.2.2 LDIF Format for Deleting Entries

When deleting an entry by using *ldapmodify* or *ldapmodifymt*, the LDIF file entry only needs the DN of the entry to be deleted and the *changetype: delete* directive. Use an empty line at the end of the entry as a separator.

```
dn: cn=Suzie Smith,ou=Server Technology,o=Acme, c=US
changetype: delete
```

The *ldapdelete* command only needs a list of DNs. It does not require a *changetype* operator.

## A.2.3 LDIF Format for Modifying Entries

When modifying an entry, you must supply the DN of the entry followed by the `changetype: modify` directive. Next you must specify the attributes you want to modify using one of the following directives:

- `add: attribute_type` - Specifies the name of an attribute type for which you want to add a value. The next line should then contain the `attribute_type: value` directive for the value you want to add. For example:

```
add: work-phone
work-phone: 510/506-7000
```

- `delete: attribute_type` - Specifies the name of an attribute type for which you want to delete the value. If the attribute is multi-valued, then you should also supply the `attribute_type: value` directive for the specific value you want to delete, otherwise all values for the attribute are deleted. For example:

```
delete: home-fax
```

- `replace: attribute_type` - Specifies the name of an attribute type for which you want to replace the existing value with a new value. The next line should then contain the `attribute_type: value` directive for the value you want to replace. For example:

```
replace: home-phone
home-phone: 415/697-8899
```

If the attribute is multi-valued then all the current values are replaced with one or more attributes following this directive. If only a single value of a multi-valued attribute needs to be replaced use `delete` then `add`.

If you are making several modifications to an entry, then, between each modification you enter, add a line that contains a hyphen (-) only. For example:

```
dn: cn=Barbara Fritchey,ou=Sales,o=Oracle,c=US
changetype: modify
add: work-phone
work-phone: 650/506-7000
work-phone: 650/506-7001
-
delete: home-fax
-
replace: home-phone
home-phone: 415/697-8899
```

## A.2.4 LDIF Format for Modifying the RDN of an Entry

To modify the relative distinguished name (RDN) for an entry, you must supply the DN of the entry followed by the `changetype: modrdn` directive. Next you must specify the new RDN with a `newrdn:` directive, and you can optionally delete or keep the old entry by supplying a `deleteoldrdn:` directive. For example:

```
dn: cn=Sally Smith,ou=people,dc=example,dc=com
changetype: modrdn
newrdn: dn=Sally Smith-Jones
# deletes old RDN entry
deleteoldrdn: 1
```

## A.2.5 LDIF Format for Modifying the DN of an Entry

To modify the DN for an entry (move the entry to a new node in the DIT), you must supply the DN of the entry followed by the `changetype: moddn` directive. You must also specify the new parent DN with a `newsuperior: directive`, and you can optionally delete or keep the old entry by supplying a `deleteoldrdn: directive`. For example:

```
dn: cn=Sally Smith,ou=people,dc=example,dc=com
changetype: moddn
# keeps old RDN entry
deleteoldrdn: 0
newsuperior: ou=expeople,dc=example,dc=com
```

## A.3 LDIF Format for Adding Schema Elements

Attribute types and object classes must be added to the Oracle Internet Directory schema before they can be used in entries.

### Example: Adding an Attribute to the Schema

This example adds a new attribute to the schema called `myAttr`. The LDIF file for this operation is:

```
dn: cn=subschemasubentry
changetype: modify
add: attributetypes
attributetypes: ( 1.2.3.4.5.6.7 NAME 'myAttr' DESC 'New attribute definition'
  EQUALITY caseIgnoreMatch SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )
```

On the first line, enter the DN specifying where this new attribute is to be located. All attributes and object classes are stored in `cn=subschemasubentry`.

The second and third lines show the proper format for adding a new attribute.

The last line is the attribute definition itself. The first part of this is the object identifier number: `1.2.3.4.5.6.7`. It must be unique among all other object classes and attributes. Next is the `NAME` of the attribute. In this case the attribute `NAME` is `myAttr`. It must be surrounded by single quotes. Next is a description of the attribute. Enter whatever description you want between single quotes. At the end of this attribute definition in this example are optional formatting rules to the attribute. In this case we are adding a matching rule of `EQUALITY caseIgnoreMatch` and a `SYNTAX` of `1.3.6.1.4.1.1466.115.121.1.15` (which is the object ID for the syntax of "Directory String").

When you define schema within an LDIF file, insert a white space between the opening parenthesis and the beginning of the text, and between the end of the text and the ending parenthesis.

### Example: Adding an Object Class to the Schema

Before you add the object class, all of the attribute types that the object class uses must be in the schema. If there are new attribute types, then define those first in your LDIF file before defining your object class.

The following example adds a new object class named `myObjectClass` to the schema.

```
dn: cn=subschemasubentry
changetype: modify
add: objectClasses
objectClasses: ( 1.2.3.4.56789.1.0.200 NAME 'myObjectClass'
  SUP ( top ) STRUCTURAL
  MUST ( cn )
```

```
MAY ( myAttr1 $ myAttr2 $ myAttr3 ) )
```

On the first line, enter the DN specifying where this new object class is to be located. All attributes and object classes are stored in `cn=subschemasubentry`.

The second and third lines show the proper format for adding a new object class.

The last line is the object class definition itself. The first part of this is the object identifier number: `1.2.3.4.56789.1.0.200`. It must be unique among all other object classes and attributes. Next is the `NAME` of the object class. In this case the object class name is `myObjectClass`. It must be surrounded by single quotes. Next is the superior (`SUP`) object classes, which in this case is `top`. `STRUCTURAL` denotes the type of object class. `MUST` and `MAY` denote the required and allowed attributes. Separate attribute names with a dollar sign (`$`).

When you define schema within an LDIF file, insert a white space between the opening parenthesis and the beginning of the text, and between the end of the text and the ending parenthesis. If using line breaks for formatting long lines, make sure to add a space at the beginning of a line to denote that it is a continuation of the previous line.

### Example: Adding A New Object Class to an Entry

Before you can use a new object class and the attributes it contains, you must update the entry to use the new object class. The following example shows how to add a new object class to an entry. Note that you must define a value for all of the required attributes of the object class.

```
# Add a new AUXILIARY object class to an existing entry
dn: cn=Robert Smith,ou=people,dc=example,dc=com
changetype: modify
# the object class used for binding
objectclass: inetorgperson
# objectclass being added
objectclass: myObjectClass
# MUST attributes of new object class
myAttr1: some value
myAttr2: my value
myAttr3: a value
```

## A.4 LDIF Format for Migrating Entries

This section describes how to properly format an LDIF file for use with the Oracle Internet Directory Migration Tool. The migration tool enables you to take LDIF entries output from other directories or applications and convert the data to use the attributes and values found in Oracle Internet Directory entries. You do this by inserting substitution variables for the data elements you want to convert.

See [Section 3.14, "ldifmigrator"](#) for more information about the Oracle Internet Directory Migration Tool.

### A.4.1 Substitution Variables for Migration Input Files

Substitution variables are denoted in the LDIF file by the following syntax:

```
%s_variableName%
```

For example, let's say you have the following LDIF formatted entry that was exported from another application. The subtree where user entries are stored, the user nickname attribute, and the name of the user's organization are different in Oracle Internet Directory than in the original application. For those elements you want to convert, you would add substitution variables to the file as placeholders.

**Example:**

```
dn: cn=jdoe, %s_UserContainerDN%
sn: Doe
%s_UserNicknameAttribute%: jdoe
objectClass: inetOrgPerson
objectClass: orclUserV2
title: Member of Technical Staff
homePhone: 415-584-5670
homePostalAddress: 234 Lez Drive$ Redwood City$ CA$ 94402
ou: %s_UserOrganization%
```

When you run the Oracle Internet Directory Migration Tool against this file, it will find the variables and either replace them with the values you define on the command-line or look up the correct values in Oracle Internet Directory.

**A.4.1.1 Predefined Substitution Variables**

The Oracle Internet Directory Migration Tool recognizes several predefined substitution variables. If running the tool in lookup mode, the values for these variables can be looked up in Oracle Internet Directory. You can use these predefined variables or define variables of your own using the `%s_variableName%` syntax.

**Table A–1** Predefined Substitution Variables

Variable Name	Meaning	How OID Migration Tool Determines the Value for This Variable
<code>%s_UserContainerDN%</code>	Distinguished name of the entry under which all users are supposed to be added.	This is assigned the value of the attribute: <code>orclCommonUserSearchBase</code> from the entry <code>cn=Common, cn=Products</code> under the realm- specific Oracle context.
<code>%s_GroupContainerDN%</code>	Distinguished name of the entry under which all public groups are supposed to be added.	This is assigned the value of the attribute: <code>orclCommonGroupSearchBase</code> from the entry <code>cn=Common, cn=Products</code> under the realm- specific Oracle context.
<code>%s_UserNicknameAttribute%</code>	The nickname attribute to be used for user entries in the identity management realm.	This is assigned the value of the attribute: <code>orclCommonNicknameAttribute</code> from the entry <code>cn=Common, cn=Products</code> under the realm- specific Oracle context.
<code>%s_SubscriberDN%</code>	Distinguished name of the LDAP entry corresponding to the identity management realm.	If a simple subscriber name is given, the migration tool will resolve it to a DN using the attribute <code>orclSubscriberSearchBase</code> and the <code>orclSubscriberNickNameAttr</code> from the entry <code>cn=Common, cn=Products</code> under the root Oracle context.

**Table A-1 (Cont.) Predefined Substitution Variables**

Variable Name	Meaning	How OID Migration Tool Determines the Value for This Variable
%s_SubscriberOracleContextDN%	Distinguished name of the realm-specific Oracle Context.	First the realm DN is computed as described earlier and then the string <code>cn=OracleContext</code> is pre-pended to it.
%s_RootOracleContextDN%	Distinguished name of the Root Oracle Context.	This is currently hard-coded to <code>cn=OracleContext</code> .
%s_CurrentUserDN%	Distinguished name of the User who is loading the LDIF file. This is sometimes required to bootstrap the creation of groups which require at least one member in them.	The migration tool expects this DN to be specified on the command line as part of the authentication information.

## A.4.2 Reconcile Options for Migrated Entries

When migrating entries into Oracle Internet Directory from another application, it is possible that there may be conflicts. For example, a user entry may already be defined in Oracle Internet Directory, or have conflicting values with the migrated data. In this case, the reconcile option will control what LDIF `changetype` directives are performed. There are three modes for reconciliation of migrated data:

- **SAFE** - This mode only adds new entries that don't exist or appends new attributes to existing entries. If any other directive besides the following are specified in the LDIF file, they will not be applied.

```
changetype:add

changetype:modify
  add: attribute_name (adds attribute only if it doesn't exist)
```
- **SAFE-EXTENDED** - This mode only adds new entries that don't exist or appends new attributes to existing entries. If you try to add a new value for existing attributes, then it will add it to the existing set of values. If any other directive besides the following are specified in the LDIF file, they will not be applied.

```
changetype:add

changetype:modify
  add: attribute_name (appends values if attribute exists)
```
- **NORMAL** - This mode applies all directives as intended. The following directives are supported:

```
changetype:add

changetype:delete

changetype:modify
  add: attribute_name
  replace: attribute_name
  delete: attribute_name
```