

Integrated Services Directory

U S E R G U I D E

InterMail Mx Version 5.1

March, 2000

Software.com[®]
THE INTERNET INFRASTRUCTURE COMPANY

Software.com, Inc.

www.software.com

525 Anacapa Street
Santa Barbara, CA 93101-1603
Tel: (805) 882-2470
Fax: (805) 882-2473

10 Maguire Road, Suite 400
Lexington, MA 02421-3130
Tel: (781) 274-7000
Fax: (781) 674-1080

The InterMail software is a copyrighted work of Software.com, Inc.
© 1993–2000 Software.com, Inc. All rights reserved.

InterMail includes software that is copyright © 1990, 1993, 1994, The Regents of the University of California. All rights reserved. This code is derived from software contributed to Berkeley by Mike Olson.

SmartHeap, portions copyright © 1991–1997, Compuware Corporation.

InterMail incorporates a derivative work of the SSL Plus: SSL 3.0 Integration Suite Toolkit, copyright © 1996, 1997, Consensus Development Corporation. SSL Plus: SSL 3.0 Integration Suite is a trademark of Consensus Development Corporation, which reserves all rights thereto.

Portions of the SSL Plus: SSL 3.0 Integration Suite Toolkit software are based on SSLRef™3.0, which is copyright © 1996, Netscape Communications Corporation. SSLRef™ was developed by Netscape Communications Corporation and Consensus Development Corporation.

The MD5 Message-Digest algorithm used in InterMail is a copyrighted work of RSA Data Security, Inc., copyright © 1991–1992, RSA Data Security, Inc. All rights reserved.

InterMail incorporates a derivative work of the BSAFE cryptographic toolkit, copyright © 1992–1996, RSA Data Security, Inc. All rights reserved.

BSAFE is a trademark of RSA Data Security, Inc.

The RSA Public Key Cryptosystem is protected by U.S. Patent #4,405,829.

The Regular Expression Routines used in InterMail are copyright © 1992–94, Henry Spencer. All rights reserved. This software is not subject to any license of the American Telephone and Telegraph Company or of the Regents of the University of California.

The InterMail LDAP code is derived from software that is copyright © 1992–1996 Regents of the University of Michigan. All rights reserved. Redistribution and use in source and binary forms are permitted provided that this notice is preserved and that due credit is given to the University of Michigan at Ann Arbor. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission. This software is provided “as is” without express or implied warranty.

The *Integrated Services Directory User Guide* is a copyrighted work of Software.com, Inc.
© 1997–2000, Software.com, Inc. All rights reserved.

No part of this documentation may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose other than personal use, without the express written permission of Software.com, Inc.

This copyrighted work contains trade secret information of Software.com, Inc. Use, transfer, disclosure, or copying without the express written permission of Software.com, Inc., is strictly forbidden. Information in this document is subject to change without notice and does not represent a commitment on the part of Software.com, Inc.

INTERMAIL, SOFTWARE.COM, and SOFTWARE.COM THE INTERNET INFRASTRUCTURE COMPANY are registered trademarks, and POST.OFFICE and WEBEDGE are trademarks, of Software.com, Inc. and are registered trademarks in various countries around the world.

NETSCAPE is a registered trademark of Netscape Communications Corporation.

OPENVIEW is a registered trademark of Hewlett-Packard Company.

WINDOWS NT is a registered trademark of Microsoft Corporation.

SQL*NET is a trademark and ORACLE is a registered trademark of Oracle Corporation.

SUN is a registered trademark of Sun Microsystems, Inc.

VERITAS is a registered trademark of Veritas Software Corporation.

Other product, brand, and company names mentioned herein may be trademarks, registered trademarks, or service marks of their respective holders.

Integrated Services Directory User Guide, InterMail Mx Version 5.1

Document number: MISD-000310

Table of Contents

Preface	vii
1: Introduction	1
Role of the ISD	1
Features of the ISD	3
Scalability Features	3
Security Features	4
Directory Data Access	4
LDAP Basics	4
LDAP Standards	6
2: Directory Server	7
Server Architecture and Information Flow	7
Read Requests	8
Read-Through Requests	8
Write-Through Requests	9
Direct Write Requests	9
Directory Access Control Information	9
Updates to the Directory Cache Database	11
Configuration Options	12
Statistics	15
3: Directory Cache Server	17
Server Architecture and Information Flow	17
Read Requests	19
Read-Through Requests	19
Write-Through Requests	19
Server Synchronization	20
File Structure	20
Server Operation	21
Directory Cache Database Initialization	21
Communications Protocols	22
RME Queries	22
LDAP Queries	23
Attribute Indexing	23
Configuration Options	24
Statistics	31
4: Replicating and Partitioning Data	35
Overview of Replication and Partitioning	35
Replication	35
Partitioning	36
Planning your Replication Design	37
Defining a Replication Agreement	39
Storage of Replication Agreements	40

Chaining Directory Cache Servers	40
Chaining Scenarios Involving Routing Lists.....	41
Configuration Keys Used for Replication Agreements.....	42
Setting Up a Replication Agreement	43
Examples of Replication Agreements.....	44
Replicating a Complete Copy of the Directory Database	44
Using a Replica Set	46
Using Chaining.....	47
Using Partitioning with Multiple Replication Agreements	50
Using Replica Sets with Partitions	53
Using Application Partitioning.....	57
5: Customizing the Directory Schema	59
Customizing Object Classes.....	60
About Object Classes	60
Abstract Object Classes	62
Structural Object Classes	62
Auxiliary Object Classes	63
Creating Object Classes.....	63
Customizing Attributes	65
About Attributes	65
Adding New Attributes.....	67
Defining a New Attribute in the Schema	68
Adding a New Attribute to an Object Class You Created Previously	69
Adding a New Class-of-Service Attribute	71
Defining Attribute Constraints	73
Schema Checking.....	74
Post-Customization Tasks.....	74
6: Customizing the DIT	77
About InterMail's Initial DIT	77
About the Administration Tree.....	79
About the Application Tree	80
Customizing DIT Entries	80
Adding Domains.....	81
Adding Organizations.....	82
Adding Organizational Units.....	83
Modifying Access Control Information Rules	84
Adding Administrative Groups	86
Adding Administrators	88
Adding Administrative Policies	89
Adding Attribute Constraints	92
Modifying Attribute Constraints	93
Modifying Class-of-Service Attributes	94
Adding COS Attributes	96
Adding Allocation Rules	96
Defining Administrative Roles.....	97
Adding Administrative Realms	98

7: Directory Schema Tables	99
Tables Defining LDAP Object Classes.....	100
adminAllocation	101
adminAllocCounts.....	102
adminGroup.....	103
adminPolicy.....	103
adminRealm.....	104
adminRealmSpec.....	105
adminRole.....	105
adminRoot	106
adminTarget.....	106
adminUserPrefs	107
alias.....	107
applicationEntity.....	107
applicationProcess	108
certificationAuthority	108
certificationAuthority-V2.....	109
changeLogEntry	109
country.....	109
cRLDistributionPoint	110
dcObject.....	110
device.....	110
dmd.....	111
domain	112
dsA.....	113
groupOfNames	114
groupOfUniqueNames.....	114
inetOrgPerson	115
locality	116
mailDomain	117
mailLocalUserPrefs	117
mailUser	117
mailUserPrefs	118
organization	120
organizationalPerson	121
organizationalRole.....	122
organizationalUnit	123
partition.....	124
person	125
replAgreement	125
residentialPerson.....	126
scConfig.....	127
scConfigRoot.....	127
subschema.....	127
top	128
userSecurityInformation	128
Tables Defining LDAP Attributes	128

8: Directory Configuration Keys	185
Sample Configuration Key.....	185
InterMail Servers and Processes.....	186
Common Server Configuration	187
Individual Server Configuration	187
Impact of Configuration Key Changes.....	187
Directory Configuration Keys.....	188
9: Directory Management Utilities	235
imaccountreport	236
imcacheread	237
imdbcontrol	238
Syntax for imdbcontrol.....	238
Available imdbcontrol Operations	239
Domain Operations	239
Account Operations	240
Mail Delivery Operations	241
SMTP Alias Operations	241
Class of Service Operations	241
Domain Operations.....	242
Account Operations	247
Mail Delivery Operations.....	260
SMTP Alias Operations.....	264
Class of Service Operations.....	266
imdirmake	268
imdirprobe	269
imdirsync.....	270
imdirupdate	270
imldapsh.....	271
imldapsh Options	272
Special Variables	276
Using imldapsh Instead of imdbcontrol	276
imldifexport.....	278
impwdhash	279
ldapadd.....	280
ldapdelete	282
ldapmodify	283
ldapmodrdn	285
ldapsearch.....	286
A: License Information	289
Glossary.....	297
Index.....	303

Preface

Welcome to the InterMail Mx Integrated Services Directory (ISD)!

The *Integrated Services Directory User Guide* contains conceptual information about the architecture of the Integrated Services Directory (ISD), directory configuration keys, the directory schema, the Directory Information Tree (DIT), and directory management utilities. It also contains procedures to help you customize the ISD architecture, schema, and DIT to meet the unique needs of your site.

Intended Audience

This guide assumes that you are experienced with the UNIX operating system at a system administration level, and that you have an understanding of databases as well as of networking protocols and related technology.

Organization

This manual is organized as follows:

- Chapter 1, Introduction, provides an overview of the role and features of the InterMail Mx ISD, and includes a brief overview of the LDAP directory data model.
- Chapter 2, Directory Server, describes the architecture and function of the InterMail server that maintains the authoritative master copy of the Directory database and is responsible for all communication with it.
- Chapter 3, Directory Cache Server, describes the architecture and function of the InterMail server that services all requests for end-user authentication and InterMail account information during message delivery, retrieval, and storage.
- Chapter 4, Replicating and Partitioning Data, provides practical guidance in planning a replication design for your site.
- Chapter 5, Customizing the Directory Schema, provides guidelines to help you extend the ISD schema for your unique application.
- Chapter 6, Customizing the DIT, provides detailed instructions to help you customize the DIT for your site.

- Chapter 7, Directory Schema Tables, defines the data that can be stored in the ISD by describing the object classes and attributes that make up the LDAP schema.
- Chapter 8, Configuration Keys, describes all configuration keys relating to the Directory server and Directory Cache server.
- Chapter 9, Directory Management Utilities, describes the syntax and usage of all ISD management commands.

Conventions

Convention	Description	Example
\$ at the start of a string	An environment variable (set at the time of installation)	\$spoolDir
monospace type	<ul style="list-style-type: none"> • Commands • Directory and file names • Hostnames • Configuration keys and their values • Utility names 	imdbcontrol command cron utility Set this key to true.
<angle brackets> in a command	A required variable	imboxget <address>
[square brackets] in a command	An optional parameter	imctrl [-verbose]
(a vertical bar) between options in a command	Exclusive options, of which you can use only one	impwdhash -a [md5-po unix]
{braces} around options in a command	A list of options, one of which is required	immsgdelete {<msgID>... -all}
. . . (an ellipsis) after an optional entry in a command	An option for which you may have multiple entries	imbucketscreate [<c1...cn>]
boldface in an example	User input	venus% imservctrl stop

Related Documentation

This manual is one of a set. Other manuals in this set are:

- *InterMail Mx Reference Guide*, which contains background information about the InterMail servers and databases, configuration keys, administrative utilities, APIs, and event messages.
- *InterMail Mx Operations Guide*, which provides instructions for the operation and administration of the InterMail system.
- *InterMail Mx Installation Guide*, which provides instructions for installing InterMail.
- *InterMail Mx Upgrade Guide*, which provides instructions for upgrading from previous versions of the InterMail product.
- *InterMail Mx Migration Guide*, which provides instructions for migrating to InterMail from the Post.Office, Sendmail, and Netscape messaging products.

Questions and Comments

Your feedback is important to us! To suggest improvements or make comments on the content of this manual, please send e-mail to InterMail.Manual@Software.com.

1

Introduction

The InterMail Mx Integrated Services Directory (ISD) is the heart of the InterMail system. It is the definitive source of all InterMail account information, and is accessed during all message delivery, message storage, and message retrieval operations. The ISD supports the Lightweight Directory Access Protocol (LDAP), which is an Internet standard for client-server interaction.

This chapter provides an introduction to the ISD. It covers:

- Role of the ISD
- Features of the ISD
- Directory data access
- LDAP basics
- LDAP standards

Role of the ISD

The ISD plays a central role in all interactions among the mail servers in the InterMail system. It provides the account information necessary for message delivery and retrieval, such as:

- Username
- Password
- E-mail address
- Mailbox identifier
- Host information

The ISD is composed of the following parts:

- Directory server
- Directory database

- Directory Cache server
- Directory Cache database

These components work together to authenticate users and to provide account information during all message delivery, storage, and retrieval operations.

Figure 1 shows the components of the ISD.

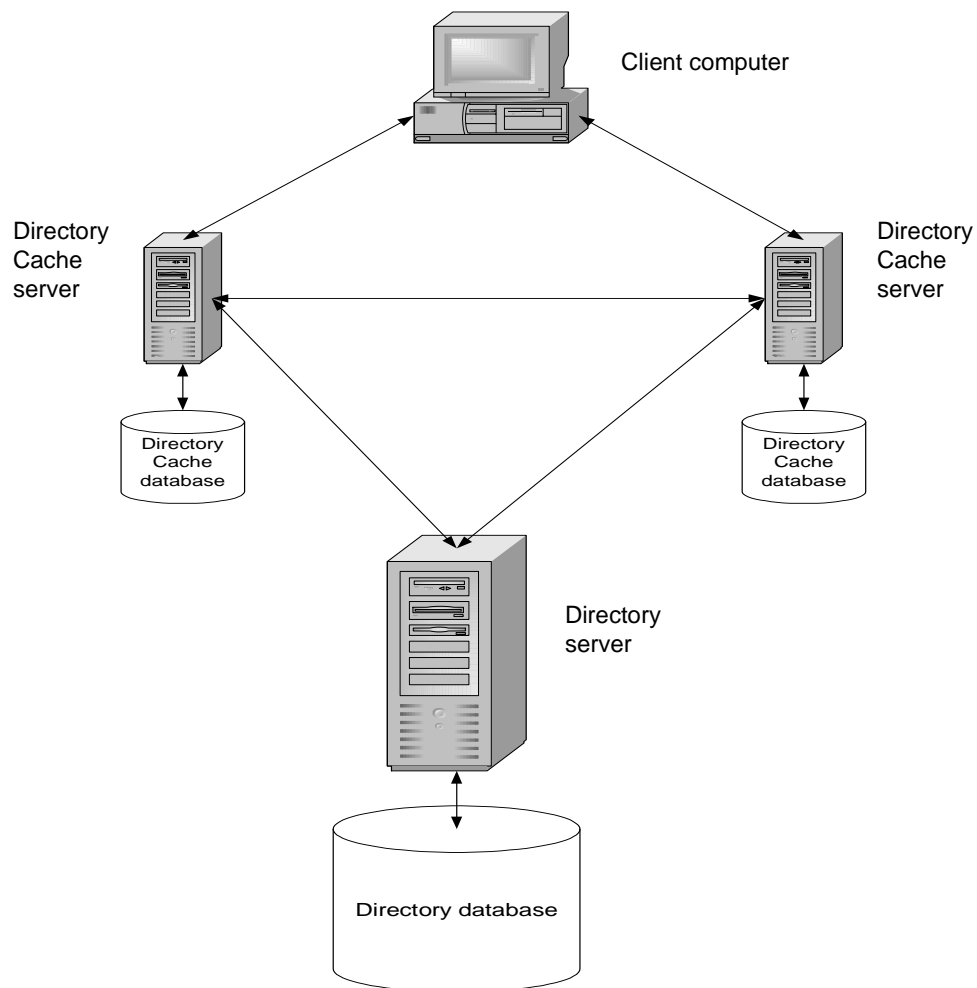


Figure 1 Components of the Integrated Services Directory

The **Directory database** is the authoritative source of all directory data.

The **Directory server** is the only server to communicate directly with the Directory database. It relays account information between the Directory database and each Directory Cache server. It can read through to the Directory database at any time to request new account information.

The **Directory Cache servers** automatically update their account information by contacting the Directory server at configurable intervals. Each Directory Cache server responds to requests for account information by checking its cache. If it cannot find

the requested information there, it reads through to the Directory server to obtain the most current information from the Directory database.

Each **Directory Cache database** contains a local copy of all or part of the Directory database.

Features of the ISD

This section introduces some important features of the ISD, including:

- Scalability features
- Security features

Scalability Features

The InterMail Mx ISD can scale efficiently to service millions of accounts. The most important contributor to the scalability of the InterMail Mx ISD is its distributed architecture, in which multiple Directory Cache servers running on local host machines communicate with a single Directory server that encapsulates the Directory database. Other contributors to the scalability of the ISD are replication and partitioning.

Distributed architecture—You can have as many Directory Cache servers as your system requires to run most efficiently, and you can add more as your organization grows. This eliminates bottlenecks to the Directory database, ensuring rapid responses to the other InterMail servers by not burdening the Directory server with read requests.

Replication—The Directory Cache servers can automatically replicate data from the Directory server, and store it in their local caches. Replication enables continuous operation if a server fails to operate. It also enables the query load to be balanced among several Directory Cache servers. Replication agreements define filters that determine which attributes and entries from the Directory database are replicated to a particular Directory Cache database. For a detailed discussion of data replication, see Chapter 4.

Partitioning—The partitioning feature enables you to designate a specific Directory Cache database and its associated server for a specific purpose. For example, you can designate individual local Directory Cache databases to hold account information for each of your regional offices. Alternatively, you can designate one Directory Cache database to hold frequently requested information and designate its server to respond to read-only queries. A replication agreement specifies which Directory Cache server maintains which database entries. For a detailed discussion of data partitioning, see Chapter 4.

Security Features

The ISD includes a number of security features. It enables you to restrict the set of IP addresses that can communicate with the Directory server or with a particular Directory Cache server, and to control whether anonymous binding is permitted.

In addition, all read and write requests to the Directory Cache servers and the Directory server go through Access Control Information (ACI) filters, which you set with LDAP commands. These filters determine whether a particular user is allowed to access or modify information in specific parts of the directory. For detailed information on ACI filters, see Chapter 2.

Directory Data Access

You can access and manipulate ISD data using command line directory management utilities and application programming interfaces (APIs). You can access and manipulate ISD servers by using configuration keys.

You can access the directory management utilities from the UNIX command line to query the ISD and to add, modify, or delete ISD data. Directory management utilities also enable you to export data from the ISD to a third-party directory, import LDIF (LDAP Data Interchange Format) data from a foreign directory into the ISD, store passwords in a hashed format, and perform other complex operations.

You can use the C and Perl API libraries to create programs that create, read, modify, or delete ISD data.

You can control the behavior of the Directory server and Directory Cache server by using configuration keys to modify the values of configuration options in the Configuration database. For information on configuration keys, see Chapter 8.

LDAP Basics

The ISD uses LDAP (Lightweight Directory Access Protocol), the Internet industry-standard protocol for remote access and integration of diverse directory services. Using LDAP eliminates the need for gateways or connectors to convert data to proprietary protocols or message formats, and it enables the Directory Cache servers to answer queries from any LDAP client or server, in addition to answering RME queries from other InterMail servers.

The LDAP-based object-oriented data model and schema allow the ISD to be easily integrated with your other applications and enable you to access and extend your existing directory schema for use with the InterMail system.

The LDAP model has eight features for performing directory-related tasks:

- Information model
- Schema

- Naming model
- Security model
- Functional model
- Protocol
- Application program interface
- LDIF (LDAP Data Interchange Format)

Each of these is described briefly below.

Information model—The LDAP information model defines the kind of data that can be stored in a directory. LDAP directories are populated with entries, which are collections of attributes and their values. For example, a directory entry representing a person named John Doe could have an attribute called `sn` (surname) with the value `Doe`.

This model is extensible, meaning that new types of information can be added to an LDAP directory. However, LDAP sets constraints on these entries so that they are compatible with other LDAP directories.

Schema—An LDAP schema is a collection of object classes and their attributes. It sets the rules for what can be stored in the directory, such as which attributes are associated with a particular object class, and the syntaxes of those attributes. It also defines the structure of the data in the Directory Information Tree (DIT).

Naming model—The LDAP naming model specifies that directory entries must be hierarchical and organized in an inverted tree structure. Each entry has a unique name, called a distinguished name (DN). The distinguished name consists of a list of the names of all the parent entries in the directory back to the directory root. The first entry typically represents the most specific name, such as the user ID, followed by the group name, followed by the company name, followed by the name at the top of the DIT. For example,

```
dn: uid=johndoe, ou=engineering, dc=software, dc=com
```

This is the opposite of operating system paths, in which the most general name comes first, and the most specific filename comes last.

Security model—The LDAP security model described how directory information is secured against unauthorized access by an authentication process called binding, coupled with a system of Access Control Information (ACI) filters.

The LDAP client provides the user's distinguished name and a password to the LDAP server. The LDAP server then locates the distinguished name in the directory and checks whether the given password matches the password stored in the directory for this client. If it matches, the client is authenticated, and the privileges granted to that user are enabled. The ACI filters are a set of rules that protect the information in the directory by specifying who can and cannot read or modify a particular entries. The Directory server enforces these rules by allowing or denying access to the specified user.

Functional model—The LDAP functional model comprises eight basic functional operations that you can perform on directory data:

- `bind` and `unbind` begin and end, respectively, the exchange of authentication information between LDAP clients and the directory server.
- `add`, `delete`, and `modify` apply to individual directory entries.
- `search` locates specific entries in the DIT.
- `compare` allows client applications to test the accuracy of information against information in the Directory database.
- `modifyRDN` allows you to change the distinguished name of an entry.

Protocol—The LDAP network protocol specifies the interaction between clients and servers and determines how LDAP queries and responses are carried over the IP network.

Application program interface (API)—The LDAP API supplies a standard set of function calls and definitions to allow customized software programs to access and interact with the directory.

LDAP Data Interchange Format (LDIF) - LDIF is an ASCII text file format used to describe directory entries and operations on those entries. It enables you to create, modify, and delete Directory entries, and to import and export data among any LDAP directories. LDIF files look like the following example:

```
dn: uid=johndoe, ou=engineering, dc=software, dc=com
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
cn: John Doe
sn: Doe
uid: johndoe
mail: johndoe@software.com
telephoneNumber: 781 123 4567
```

The technical specification for LDIF can be found at <http://search.ietf.org/internet-drafts/draft-good-ldap-ldif-05.txt>.

LDAP Standards

The LDAP models and protocols are set out in a series of Internet Engineering Task Force (IETF) Requests for Comments (RFC) and Internet Drafts. These may be found on the IETF Web site <http://www.ietf.org>.

The IETF is an international organization of network researchers and designers who work on improving Internet architecture and Internet protocols.

The LDAP protocol, version 2, is specified in RFCs 1777-1779, 1823, and 1960. LDAP version 3, which is the latest version of the protocol, is specified in RFCs 2251-2256.

2

Directory Server

The Directory server, a component of the Integrated Services Directory (ISD), maintains an authoritative master copy of the Directory database. The Directory server is the only client of the Directory database; as such, the Directory server is responsible for all write requests to the Directory database, as well as for storage of replication information that is read by the Directory Cache servers. For detailed information on the Directory Cache servers, see Chapter 3; for information on replication, see Chapter 4.

This chapter covers:

- Server architecture and information flow
- Directory access
- Updates to the Directory Cache database
- Server configuration options
- Server statistics

Server Architecture and Information Flow

The Directory server (process name `imdirserv`) communicates with the Directory database by means of the SQL*NET protocol, and with the Directory Cache servers and remote clients by means of the LDAP protocol.

The Directory server contains application intelligence logic to ensure that database provisioning rules are enforced as the Directory database is modified. These provisioning rules dictate, for example, that each SMTP address must be unique and its domain be represented by an entry, that each domain rewrite rule must reference a valid domain, and so on. Provisioning rules are described in Chapter 7.

In addition, all read and write requests to the Directory server go through Access Control Information (ACI) filters, which determine whether the user making the request is allowed to access or modify information. ACI rules are described in “Directory Access Control Information” on page 9.

Figure 2 illustrates, and the following text describes, how information flows through the Directory server. The numbered steps in the text correspond to the numbers in the figure.

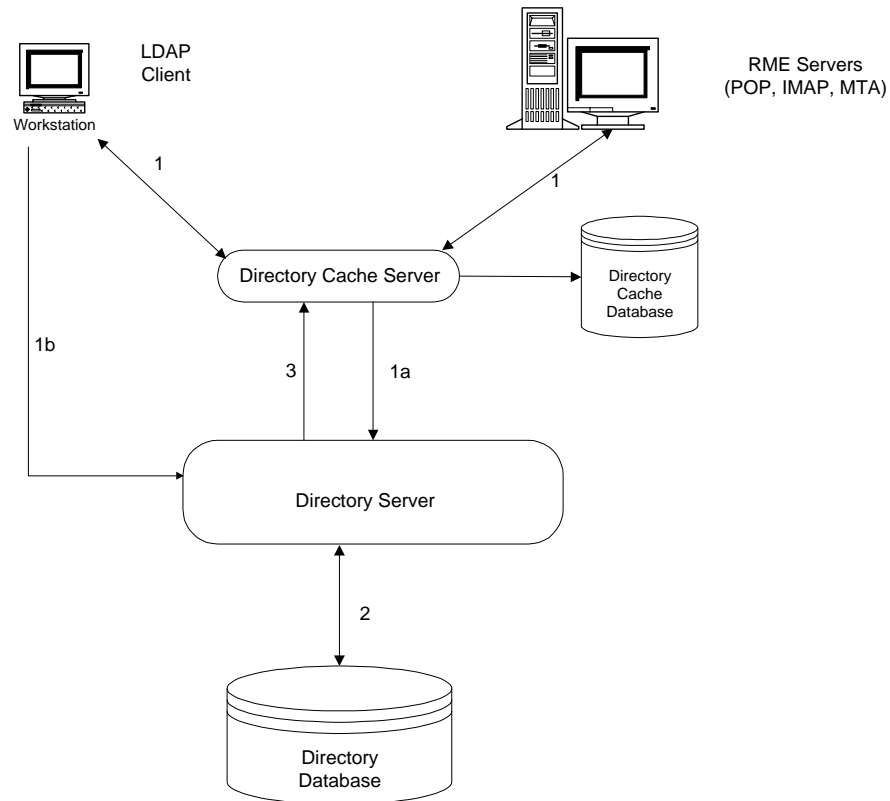


Figure 2 Information flow through the Directory server

Read Requests

The flow for read requests (Figure 2) is as follows:

1. Under normal conditions, the Directory Cache server answers read requests from a client, thus lightening the load on the Directory server.

Read-Through Requests

Read-throughs apply only to RME clients. The flow for read-through requests (Figure 2) is as follows:

1. (a) The Directory Cache server can be configured to read through to the Directory server under the following conditions:
 - The RME client requests an entry that is not present in the Directory Cache database.

- An authentication request to the Directory Cache server fails.

The Directory Cache server contacts the Directory server.

2. The Directory server contacts the Directory database using the SQL*NET protocol to obtain the requested information.
3. The Directory server relays the information to the Directory Cache server.

Write-Through Requests

The flow for write-through requests (Figure 2) is as follows:

1. (a) The Directory Cache server contacts the Directory server using the LDAP protocol.
2. The Directory server updates the Directory database.

Direct Write Requests

Clients adding or updating large numbers of accounts are typically configured to bypass the Directory Cache server and communicate directly with the Directory server. This is done for efficiency in provisioning large numbers of accounts.

The flow for direct write requests to the Directory server is as follows:

1. (b) A remote LDAP client contacts the Directory server directly using the LDAP protocol.
2. The Directory server updates the Directory database.

Directory Access Control Information

The Directory server protects the information in the Directory database by enforcing Access Control Information (ACI) rules, which specify who can and cannot read or modify a given entry.

Each ACI rule is stored in the Directory schema as an attribute of the entry to which it applies, and has the following components:

- Identity of the user or group of users accessing the data
- Directory objects the user or group can access
- Permissions

Identity of the user: The user or group of users whose access is being defined is identified by a bind distinguished name (`bindDN`), which uniquely identifies the entry in the LDAP directory, and by a bind type (`bindType`), which could be a person, an organizational unit, or any other administrative group.

Directory objects: The directory objects for which access is being defined can include entries and attributes, each represented by a target distinguished name (`targetDN`).

Permissions: The access rights that the user has for the specified directory objects can include read access (ar), write access (aw), and the administrative right to delegate read or write access to another user (aar and aaw, respectively).

Usage

acirule:<bindDN,bindType,objectClass,attribute,realm,permissions>

Where:

bindDN	<p>Is a distinguished name that uniquely identifies the user in the directory. A null value (" ") indicates all users.</p> <p>Example 1: cn=John Doe,ou=engineering</p> <p>Example 2: ou=documentation</p>
bindType	<p>Can be you, a group, or a subtree of the DIT.</p> <p>Values:</p> <ul style="list-style-type: none">selfgroupsubtree
objectClass	<p>Is the object class in the Directory schema that you want to access. A null value (" ") indicates all object classes.</p> <p><i>Note:</i> For a list and description of InterMail object classes, see Chapter 7.</p> <p>Example 1: person</p> <p>Example 2: organizationalUnit</p>
attribute	<p>is the attribute in the Directory schema that you want to access. A null value (" ") indicates all attributes.</p> <p><i>Note:</i> For a list and description of InterMail attributes, see Chapter 7.</p> <p>Example 1: userPassword</p> <p>Example 2: telephoneNumber</p>
realm	<p>Specifies whether the rule applies only to the entry specified, or also to all of its child entries.</p> <p>Values:</p> <ul style="list-style-type: none">entrychildren <p><i>Note:</i> Children are entries at a lower level in the DIT than the specified entry.</p>

permissions	Are the access rights to be allowed or denied.
	Values:
	ar allows read access only
	aw allows write access only
	aar allows the right to delegate read access to another user
	aaw allows the right to delegate write access to another user

Example 1

The following example would allow John Doe in the engineering department to read and change his own password:

```
acirule:<cn=John Doe, ou=engineering, self, "", userPassword, entry,
ar+aw>
```

Example 2

The following example would allow all the members of the documentation group to read all of the telephone numbers in the Directory, although they could not change any of them:

```
acirule:<ou=documentation,group,"",telephoneNumber,children, ar>
```

Example 3

The following example would allow anonymous read access to all object classes and attributes the Directory:

```
acirule:<"",subtree,"","",children,ar>
```

Updates to the Directory Cache Database

The Directory server maintains a change log that is read by the Directory Cache servers to update their Directory Cache databases. This log contains all additions, deletions, and modifications made to the Directory database over the period of time set by the `logAgeHours` configuration key. The Directory Cache server uses an update thread to keep track of the last change number it read from the change log in its most recent update cycle.

You control the configuration of the change log through the following keys:

- `/*/imdirserv/changeLog`
- `/*/imdirserv/expChgLogCommitSize`
- `/*/imdirserv/ldapBackend`
- `/*/imdirserv/logAgeHours`
- `/*/imdirserv/logExpireHours`
- `/*/imdirserv/writeChangeLog`
- `/*/imdirserviceserv/chgLogPageSize`

Configuration Options

The following configuration keys are useful for controlling or modifying the behavior of the Directory server. For a further discussion of these keys, as well as for information on configuration keys that can be applied to all servers, see Chapter 8.

Configuration Key Name	Description
changeLog	Specifies the distinguished name where the change log entries are stored. Caution! Do not change this key once you have set up your database. You could lose changes that are in the old change log.
createEntryAudit	Is a flag that indicates whether operational attributes (<code>createTimestamp</code> and <code>creatorsName</code>) are to be created for audit purposes for every LDAP entry.
defaultChangelogTablespace	Indicates that <code>IM_CHGLG_YYYYMMDDHHMMSS</code> tables are to be stored in a tablespace other than the one installed by the InterMail Oracle installation utility.
dirRMEPort	Is the number of the port on which the Directory server listens for RME requests.
expChgLogCommitSize	Specifies the maximum number of changelog entries stored in the Oracle rollback segment storage area after they are deleted. When this number is reached, the deletions become permanent.
ldapAllocRootOverride	Determines whether allocation maximums can be overridden by a user logged in as the root distinguished name.
ldapAllocRuleDN	Specifies the distinguished name for the entry containing the allocation rules for the InterMail administrator.
ldapMaxBatchOperations	Specifies the maximum number of operations that can be run in batch mode before an automatic commit is performed. This configuration key is used in batch mode as a safeguard against clients that do not issue <code>flush</code> requests regularly, thereby causing server-side resource utilization to grow without bounds.
ldapCosCacheMaxCount	Defines the maximum number of COS constraint sets kept in the memory cache.

Configuration Key Name	Description
ldapCosCacheMaxSizeKB	Specifies the maximum size, in kilobytes, of the COS constraint memory cache.
ldapSchemaCheck	Specifies whether newly added or modified objects are validated against the LDAP schema.
logAgeHours	Specifies the number of hours that entries will be kept in the change log before being automatically deleted.
logExpireHours	Specifies the number of hours that entries will be kept in the change log before being automatically deleted.
logNumTablesLimit	Specifies the maximum number of IM_CHGLOG_YYMMDDHHMMSS tables the Directory server maintains in the database at steady state.
maxCursorsPerConn	Defines the maximum number of database cursors that a connection can retain between LDAP operations.
modifyEntryAudit	Indicate whether operational attributes (<code>modifyTimestamp</code> and <code>modifiersName</code>) are to be created for audit purposes for every LDAP entry.
oracleConnectWait	Defines the timeout period, in seconds, for an operation waiting to obtain an Oracle connection.
primaryDbNumConnections	Defines the number of Oracle connections in the pool available for LDAP operations. <i>Note: For Oracle licensing purposes, the backend also uses one permanent connection for bookkeeping.</i>
writeChangeLog	Indicates whether changes to the LDAP directory are to be logged in the change log. <i>Note: This must be set to true to enable replication.</i>
/*/imdbcontrol/ defaultDirServer	Specifies the LDAP server (either the Directory server or the Directory Cache server) to which <code>imdbcontrol</code> connects if the host and port are not specified on the command line. This is an <code>imdbcontrol</code> key.

The following configuration keys are common to both the Directory server and the Directory Cache server and are described in Chapter 3, where the Directory Cache server is fully described.

- `anonBindAccess`
- `attributeAliasingEnable`
- `defaultDirServer`
- `dirRmeConnections`
- `dirRmeMaxSecondaryCalls`
- `initIndicesFallback`
- `ldapAccessList`
- `ldapACICacheMaxCount`
- `ldapACICacheMaxSizeKb`
- `ldapAsyncOperation`
- `ldapAsyncSearch`
- `ldapBackend`
- `ldapBatchTimeoutMs`
- `ldapClientTimeout`
- `ldapConfigDn`
- `ldapEnableAutoAdminGroup`
- `ldapEntryCacheMaxCount`
- `ldapEntryCacheMaxSizeKb`
- `ldapIndices`
- `ldapIndicesConfigRdn`
- `ldapOperationLimit`
- `ldapPort`
- `ldapRootDN`
- `ldapRootPwd`
- `ldapSchemaDn`
- `ldapSchemaFile`
- `ldapSizeLimit`
- `ldapTimeLimit`
- `numLdapConnections`

- partition
- rootBindAccess

Statistics

Statistics files contain information about system performance. The Directory server writes the following statistics to `imdirserv.stat`:

Event	Description
StatChgLogEntries	Net number of change log entries added to or removed from the Oracle change log table since the Directory server was started.
StatOracleAttrNames	Number of attribute names used in the Oracle index tables.
StatOracleConnect	Number of Oracle connections or reconnections performed by the Directory server since it was started. <i>Note: This is not the number of connections currently open.</i>
StatOracleCursors	Number of Oracle cursors currently in use by the Directory server. This can be used to measure the load on and resource requirements of this server.
StatOracleEntFetchs	Number of entries fetched from the Oracle database.
StatOracleEntries	Net number of entries added to or deleted from the Oracle database since the Directory server was started.
StatOracleEntWrites	Number of entries written to the Oracle database. This includes new entries as well as updates of existing entries.
StatOracleIdxFetchs	Number of cursor fetches by the Directory server from the Oracle index tables. <i>Note: A single fetch may return more than one row.</i>
StatOracleIdxRowsFetched	Total number of rows fetched from the Oracle index tables. <i>Note: Compare this number with StatOracleIdxFetchs to get the average number of rows retrieved per fetch.</i> <i>Compare this number with StatOracleIdxWrites to get the ratio of writes to reads.</i>
StatOracleIdxWrites	Number of inserts or updates made by the Directory server.

All statistics reported in `imdircacheserv.stat` for the Directory Cache server are also reported in `imdirserv.stat` for the Directory server. These statistics are listed in Chapter 3.

3

Directory Cache Server

The Directory Cache server, a component of the Integrated Services Directory (ISD), services all requests for end user authentication and InterMail account information during message delivery, retrieval, and storage. It contains a copy of all or part of the Directory database in its local Directory Cache database, and is capable of servicing the same read and write requests as the Directory server.

An InterMail Mx system can contain as many Directory Cache servers as necessary, although only one can reside on any single host machine.

This chapter covers:

- Server architecture and information flow
- Server synchronization
- File structure
- Server operation
- Server configuration options
- Server statistics

Server Architecture and Information Flow

The Directory Cache server (process name `imdircacheserv`) communicates with remote clients and with the other components of the ISD by means of the LDAP protocol. It communicates with the InterMail POP, IMAP, and Message Transport Agent (MTA) servers by means of the RME protocol.

The Directory Cache server modifies account information in its local cache by communicating with the Directory server to receive updates from the Directory database.

You can configure a Directory Cache server to be authoritative or non-authoritative. In authoritative mode, no read-throughs to the Directory server are allowed. In non-

authoritative mode, a read-through to the Directory server takes place whenever the requested information is not found in the local cache.

Replication and partitioning can be used together to ensure continuous operation when a server or host machine is temporarily out of service.

Directory information can be replicated on several host machines. The Configuration database stored on each host contains a list of all hosts on which Directory Cache servers run. When queried by a client, the host initially tries the first entry on its list (the primary Directory Cache server). If communication with this server fails, the host goes to the next one on the list, and so on, until it finds one that is active. For a detailed discussion of replication, see Chapter 4.

In addition, directory information can be partitioned among multiple caches residing on different hosts. Partitioning enables directory data to be distributed by geographic location, by organization, by function, by frequency of use, or by any other means you choose. For a detailed discussion of partitioning, see Chapter 4.

The Directory Cache server stays current with the Directory server using an update thread that reads change logs from the Directory server. The Directory Cache database stores a change number that determines the last change applied in the previous update cycle.

Figure 3 illustrates, and the following text describes, how information flows through the Directory Cache server. The numbered steps in the text correspond to the numbers in the figure.

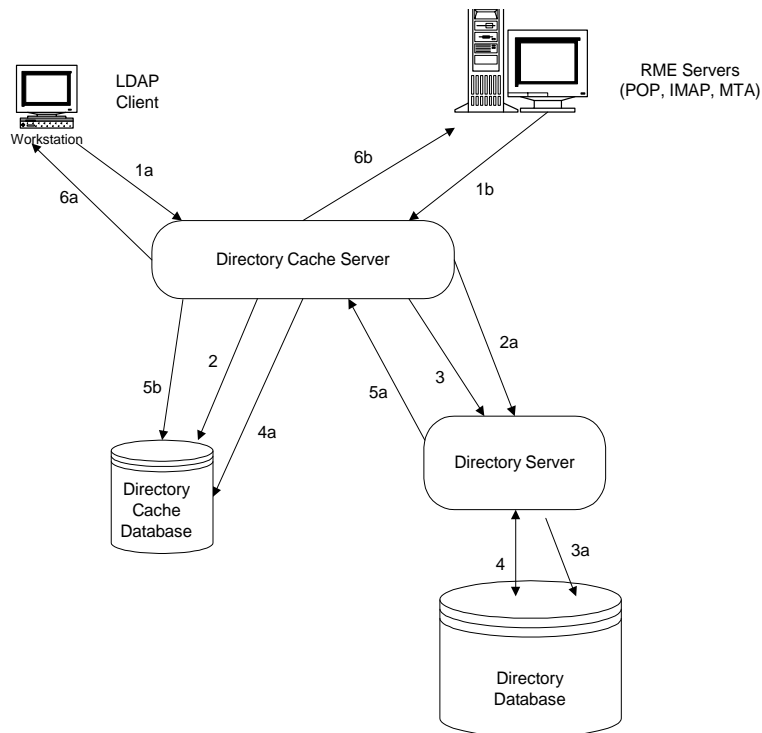


Figure 3 Information flow through the Directory Cache server

Read Requests

The flow for read requests (Figure 3) is as follows:

1. (a) A remote client using the LDAP protocol or (b) an InterMail server using the RME protocol (and thus acting as an RME client) contacts the Directory Cache server.
2. The Directory Cache server checks its local Directory Cache database for the requested information. If it finds the information, it returns it to the LDAP client (6a) or RME client (6b).

Read-Through Requests

A request reads through from the Directory Cache server to the Directory server if it comes from an RME client and any of the following conditions are true:

- The account information requested is not in the Directory Cache database.
- The account has any status other than `Active`.
- The password supplied does not match the account password.

The Directory server retrieves the latest account information from the master Directory database.

The flow for read-through requests (Figure 3) is as follows:

1. (b) An InterMail server using the RME protocol (and thus acting as an RME client) contacts the Directory Cache server.

Note: Read-through operations do not occur for LDAP clients.

2. The Directory Cache server checks its local Directory Cache database for the requested information.
3. If the Directory Cache server does not find the information requested, it contacts the Directory server.
4. The Directory server consults the Directory database to obtain the information.
5. The Directory server (a) relays the information to the Directory Cache server, which (b) updates its local Directory Cache database with the new information.
6. (b) The Directory Cache server returns the information to the RME client. If the information was not found, the Directory Cache server sends a lookup failure message to the RME client.

Write-Through Requests

The flow for write-through requests (Figure 3) is as follows:

1. (a) A remote client using the LDAP protocol contacts the Directory Cache server.
2. (a) The Directory Cache server contacts the Directory server, using LDAP.

3. (a) The Directory server writes the new information to the Directory database.
4. (a) The Directory Cache server writes the new information to its local Directory Cache database.

Server Synchronization

The Directory Cache server is synchronized with the Directory server as follows:

1. Using the LDAP protocol, the Directory Cache server updates the Directory server at configurable intervals, such as every 60 seconds.
2. The Directory server retrieves updates of all changes since its previous request from the master Directory database.
3. Using LDAP, the Directory Cache server retrieves the new information from the Directory server.
4. The Directory Cache server writes the new information to its local Directory Cache database.

File Structure

The Directory Cache server contains the following directories:

- **entry**, which contains all the latest LDAP entry data.

The `entry` directory contains the subdirectories 0, 1, 2, 3, and so on, the number of subdirectories being configurable with the `ldapNumEntryDbFiles` configuration key. Each subdirectory contains a `db` file and a `log` file.

The `db` file is the Directory Cache database. The `log` file is created as the Directory cache database is modified. Log files are numbered consecutively as they are created until a checkpoint is reached, causing the oldest files to be deleted. This checkpoint is set with the `dbLogFileMaxSizeKb` configuration key.

- **entry.old**, which holds the previous `entry` directory, replaced when the Directory Cache database was last synchronized with the Directory database.
- **index**, which contains the attribute indexing information. Attribute indexing is discussed later in this chapter.

The `index` directory contains a subdirectory for each indexed attribute, such as `acirule`, `adminpolicydn`, `cn`, `dn`, `domainname`, and so on. Each of these indexed attribute subdirectories contains another layer of subdirectories, called 0, 1, 2, 3, and so on, the number of subdirectories being configurable with the `ldapNumIndexDbFiles` configuration key. Each numbered directory contains a `db` file and a `log` file similar to those in the `entry` directory.

- **index.old**, which holds the previous generation of index information, replaced when the Directory Cache database was last synchronized with the Directory database.

Server Operation

This section covers:

- Directory Cache database initialization
- Communications protocols
- Attribute indexing

Directory Cache Database Initialization

Each host that runs a Directory Cache server maintains a local Directory Cache database in Berkeley db format.

You can initialize the Directory Cache databases by doing either of the following:

- Using the `imdirmake` and `imdirsync` utilities to:
 - Create and initialize a new Directory Cache database with the `imdirmake` command

Caution! The `imdirmake` command does not preserve existing data. Use with caution.

- Copy Directory database information from the Directory server using the `imdirsync` command
- Copying the Directory Cache database from another, active Directory Cache server. This involves:
 - Shutting down the source Directory Cache server using the `imservctrl` utility. For more information on this command, see the list of general administration utilities in the *InterMail Mx Reference Guide*.
 - Making a tarball of the `$INTERMAIL/db/entry` and the `$INTERMAIL/db/index` directories on the source Directory Cache server.

```
tar cvpf entry.tar $INTERMAIL/db/entry
tar cvpf index.tar $INTERMAIL/db/index
```

Note: You may restart the source Directory Cache server after you complete this step.

- Moving the files to the new Directory Cache server using FTP.

Note: The supplier (source) Directory Cache server and the consumer (destination) Directory Cache server must have the exact same replication agreement; that is, they must manage the exact same data in order for this operation to be successful. For more information on replication agreements, see Chapter 4.

- Untarring the files on the new Directory Cache server.

```
tar xvpf /$INTERMAIL/db/entry
tar xvpf /$INTERMAIL/db/index
```

- Starting the Directory Cache server using the `imservctrl` utility.

For more information on directory management utilities, see Chapter 9.

Communications Protocols

The InterMail servers communicate with the Directory Cache servers through an RME protocol interface. They communicate with third-party programs through the LDAP protocol.

RME Queries

The RME (Remote Method Execution) protocol is a high-performance, extensible object-oriented communications protocol used for InterMail component integration. It is not available as a public interface. RME is typically used for read-only access to the ISD. The most common RME requests to a Directory Cache server are for the server to:

- Look up account information
- Authenticate a login

Both of these requests are handled by a single RME query, which sends the primary SMTP address, the POP/IMAP username, or an SMTP alias.

A successful query returns the “Success” status along with the requested account information. Unsuccessful queries, which return no information, can have these statuses:

- Bad password
- Non-existent account
- Account in maintenance mode
- Account locked

Alias queries, which are requests for the account information for a specific alias, return success only if the supplied address is an SMTP alias or the primary SMTP address. Primary SMTP queries and POP queries return success only if the supplied address is a primary SMTP address or a POP address, respectively.

When a query to a non-authoritative Directory Cache server fails, either because the information is not in the Directory Cache database or because the password is incorrect, the Directory Cache server reads through to the Directory server. If it finds newer information, it updates the Directory Cache database with that information. This means that a query to a non-authoritative Directory Cache server never fails because of out-of-date information.

The Directory Cache server is multi-threaded. Each RME query uses its own thread, creating threads dynamically for new connections, and destroying them when connections close.

LDAP Queries

LDAP (Lightweight Directory Access Protocol) is the Internet industry standard for directory access and integration. The ISD complies with LDAPv3 standards, which may be found in RFC 2251 through RFC 2256 at <http://www.rfc-editor.org/rfcsearch.html>. All InterMail directory data is accessible through the object-oriented LDAP data model, which supports extensible object types. For a description of the LDAP data objects stored in the ISD, see Chapter 7.

A client accesses the ISD by communicating with the Directory Cache server or the Directory server, depending upon the configuration selected with the `/*/imdbcontrol/defaultDirServer` configuration key. There is no direct access to the master Directory database. The Configuration database specifies a list of preferred servers a client will contact, in order of preference. If communication fails to the first server on the list, the communication libraries automatically fail over to the next available server and continue to operate.

Users of LDAP clients access the Directory database through the InterManager GUI, the `imldapsh` command, or the LDAP API. Chapter 1 describes these methods of accessing Directory data.

Attribute Indexing

Indexing attributes improves the efficiency of directory searches by eliminating the need for the Directory Cache server to scan the entire database. You use the `ldapIndices` configuration key to index attributes that you intend to use in searches, listing the LDAP attributes to be indexed and the index type. The Directory Cache server then builds the index for you.

The syntax for the `ldapIndices` key is as follows:

```
/*/imdircacheserv/ldapIndices: [attributeName indexType]
```

There are several types of attribute indexes (`indexType`):

- The **equality index (eq)** is the most efficient index type. For a search to be successful, the exact value of the specified string must be matched. For example, if you specify `/*/imdircacheserv/ldapIndices: [mail eq]`, an SMTP address such as `mail = john.doe@software.com` would be returned only if every character matched your search query.

- The **reverse index (reverse)** searches attributes in reverse, matching their suffixes. It is useful with strings containing wildcards. For example, if you specify `/*/imdircachserv/ldapIndices: [mail reverse]` and then search for all addresses with the suffix `software.com`, the suffix is matched first, and all attributes with `mail = *@software.com` would be returned.
- The **unique index (unique)** matches attributes for which all values are unique for each entry, as in a primary SMTP address. This can be used to prevent entries containing the same attribute-value pairs from being created more than once. For example, you want each user to have a unique SMTP address, such as `mail = john.doe@software.com`. If you specify, `/*/imdircachserv/ldapIndices: [mail eq,unique]`, the Directory Cache server lists all `mail=<*>` entries in the Directory Cache database. You can look at these to ensure that you do not assign the same address to more than one person.
- The **presence index (pres)** determines whether or not an attribute is present in an entry, no matter what its value is. For example:
`/*/imdircachserv/ldapIndices: [mail pres]`
- The **approximate index (approx)** matches strings phonetically. For example:
`/*/imdircachserv/ldapIndices: [mail approx]`
- The **substring index (sub)** searches for patterns in strings. For example, `/*/imdircachserv/ldapIndices: [mail eq,sub]` would return successful searches on all users at `software.com` with the partial name “j doe”:
`mail = j*.doe@software.com`

Configuration Options

The following configuration keys are useful for controlling or modifying the behavior of the Directory Cache server. Keys marked with a plus sign (+) also apply to the Directory server. For further discussion of these keys, and for information on configuration keys that can be applied to all servers, see Chapter 8.

Configuration Key Name	Description
<code>anonBindAccess</code> +	Determines which users can have anonymous bind access, which allows them to log in and authenticate without providing a password.
<code>attributeAliasingEnable</code> +	Is a flag that enables you to use an alias for the name of a Directory database attribute. This is useful if your application has a different name for an attribute that has the same function as an InterMail Directory database attribute.

Configuration Key Name	Description
attributeSelection	Groups together attributes used by a specific directory application. This key is used to select particular attributes during replication.
cacheAlwaysReadThru	Specifies whether the Directory Cache server always reads through to the Directory when looking for account information, instead of first reading from the local cache.
cacheAuthoritativeForMTA	Specifies whether information in the Directory Cache database is considered authoritative for account queries from the MTA.
cacheAuthoritativeOnDbFail	<p>Specifies whether the Directory Cache server is considered authoritative or non-authoritative.</p> <p>If it is authoritative, it operates independently of the Directory server, even when lookups fail in its local Directory Cache database.</p> <p>If it is non-authoritative, a lookup failure results in a read-through to the Directory server to search for the information in the master Directory database.</p>
cacheDisableReadThrus	<p>Specifies whether read-throughs to the master Directory database are disabled, causing the Directory Cache server to be the authoritative source of information.</p> <p>This key takes precedence over the <code>cacheAuthoritativeForMTA</code> and <code>cacheAuthoritativeOnDbFail</code> configuration keys.</p>
cacheDisableWriteThrus	<p>Specifies whether write-throughs to the master Directory database are disabled, causing the Directory Cache server to be the authoritative source of information.</p> <p>If this key is set to <code>true</code>, no write-throughs to the Directory server take place.</p>
cacheReReadInterval	Specifies the number of seconds the system is to wait before checking to see if the cache needs to be switched. The cache needs to be switched if <code>imdirsync</code> is run to create a new cache.

Configuration Key Name	Description
chainingInfo	Provides the names of Directory Cache servers to be contacted by an index Directory Cache server to answer a request from an RME client. Maps the replication area specification specified by <code>replAreaSpec</code> to the host serving that specification.
checkPointInterval	Specifies the time interval, in seconds, between runs of the checkpoint thread. Data is written to the disk at these intervals so that it will be available in the event of a server crash.
checkPointRetryInterval	Represents the number of seconds the system should wait before retrying a checkpoint that has failed (typically, when <code>txn_checkpoint</code> returns <code>DB_INCOMPLETE</code>).
chgLogPageSize	Defines the number of entries to be read from the change log at one time.
dbLogFileMaxSizeKb	Defines the maximum size of a database log file, which is used for crash recovery.
dbSuppressFsync +	Controls whether the cache files and cache file logs will synchronize when modified.
defaultBindDN	Specifies the distinguished name used by tools such as <code>imdbcontrol</code> and API that cannot bind to the LDAP server but need communicate with the Directory Cache server.
defaultBindPassword	Specifies the password used with the configuration key <code>defaultBindDN</code> .
dirCachePort	Defines the port number on which the Directory Cache server listens for RME requests.
dirRmeConnections +	Specifies the size of the connection pool between the Directory Cache server and the other InterMail servers.
dirRmeHost	Specifies the name of the host running the Directory Cache server in builds using only one Directory server.

Configuration Key Name	Description
dirRmeHosts	Lists the hosts that are running the Directory Cache server where the RME port is available for use.
dirRmeMaxSecondaryCalls +	Caution! This key should be modified only with vendor and/or technical support.
indexThreadSnoozePeriod	Specifies the number of seconds the index thread should wait before checking to see if it needs to create additional indexes.
initIndicesFallback +	Specifies whether the server should read index information from the Configuration database during Directory Cache database initialization if an index entry in the Directory database is corrupted. If this key is set to <code>false</code> , an error message appears and the server is not initialized.
ldapAccessList +	Lists the IP addresses allowed to connect to the LDAP server. A value of <code>0.0.0.0</code> means all IP addresses are allowed.
ldapACICacheMaxCount +	Specifies the maximum number of target entries in <code>ACIGlobalCache</code> .
ldapACICacheMaxSizeKB +	Specifies the size limit of the ACI rules stored in <code>ACIGlobalCache</code> .
ldapAsyncOperation +	Enables/disables full asynchronous operation. In full asynchronous operation, a single LDAP connection can perform multiple operations at the same time. Each operation is executed in a separate thread, allowing operations to overlap. Note: If asynchronous operations are used, you must ensure that entry dependency constraints are met. For example, a parent entry must be created before you can begin an operation that creates a child entry.
ldapAsyncSearch +	Enables/disables asynchronous search operations. In asynchronous mode, a single LDAP connection can perform multiple searches simultaneously. Each search request is executed in a separate thread, allowing the searches to overlap.

Configuration Key Name	Description
ldapBackend +	<p>Caution! Do not change the value of this key without first consulting your InterMail vendor.</p> <p>Specifies the backend databases run by the server. These can be the Oracle database (ora) and/or the Oracle change logs (orachglog).</p> <p>Note: If the directory is split up among multiple backends, the portions of the DIT in the listed backends should not overlap. The code chooses the backend databases in the order listed. If there is overlap in the portions of the DIT that the backends hold, and you list a more generic suffix first, the other backends will never be called.</p>
ldapBatchTimeoutMS +	<p>Specifies the timeout period, in milliseconds, that a server in batch mode will wait before doing an automatic commit of the requests it has received.</p>
ldapBindThruEnable	<p>Enables/disables the binding of a Directory Cache server to the master when the bind distinguished name object is not found locally.</p>
ldapClientTimeout +	<p>Specifies the idle client connection timeout value.</p>
ldapConfigDn +	<p>Specifies the distinguished name of the configuration node in the LDAP directory.</p> <p>Caution! Do not change this value without consulting your InterMail vendor.</p>
ldapDbEntryCacheSizeInKB	<p>Defines the size, in kilobytes, of the database cache for the LDAP entries.</p>
ldapDbEntryPageSizeInKB	<p>Specifies the database page size, in kilobytes, for the LDAP entries in the Directory Cache server.</p>
ldapDbIndexCacheSizeInKB	<p>Defines the size, in kilobytes, of the database cache for the LDAP indices.</p>
ldapDbIndexPageSizeInKB	<p>Specifies the page size, in kilobytes, for the LDAP index database.</p>

Configuration Key Name	Description
ldapDebugWriteEnable	Enables/disables the Directory Cache server debug mode. In this mode, data is written directly to the cache, with no write-through to the Directory server.
ldapEnableAutoAdminGroup +	Specifies whether the system tries automatically to determine if the user attempting to bind to a server belongs to an InterManager administration group. If so, it enables the corresponding InterManager group privileges.
ldapEntryCacheMaxCount +	Specifies the maximum number of LDAP entries in the entry cache. (The entry cache is an in-memory cache on top of the Sleepycat database cache.)
ldapEntryCacheMaxSizeKb +	Specifies the maximum size of LDAP entries in the entry cache.
ldapIndices +	Lists LDAP attributes to be indexed for the Directory Cache server, and how they are to be indexed. You must index all instances of the attribute, since there is no means of limiting the index to a particular object class. <i>Note: The Directory Cache server builds the index for you. You do not have to run a utility to build the index.</i>
ldapIndicesConfigRdn +	Specifies the relative distinguished name of the indices' storage node.
ldapMasterHosts	Lists the hosts on which the master Directory server is running.
ldapNumEntryDbFiles	Specifies the number of files comprising the LDAP entry database.
ldapNumIndexDbFiles	Specifies the number of files comprising the LDAP index database.
ldapOperationLimit +	Defines the number of allowable LDAP client operations per connection.
ldapPort +	Specifies the number of the port on which the Directory server or Directory Cache server listens for LDAP requests.

Configuration Key Name	Description
ldapReplicationAgreement	Lists the replication agreements for the server.
ldapRootDn +	Specifies the root distinguished name for the server. <i>Note: Do not set this configuration key on a per-host basis. To change the key, modify only the <code>/* /common/ldapRootDN</code> version of the key, and then restart all Directory servers.</i>
ldapRootPwd +	Specifies the password for the root entry on the server. <i>Note: Do not set this configuration key on a per-host basis. To change the key, modify only the <code>/* /common/ldapRootPwd</code> version of the key, and then restart all Directory servers.</i>
ldapSchemaDn +	Specifies the distinguished name of the schema entry. Once the data is provisioned, this key should not be changed.
ldapSchemaFile +	Specifies the path of the schema <code>config</code> file. Paths are either absolute or relative from <code>\$INTERMAIL</code> . Schema changes must be made with care, according to the documented guidelines.
ldapServerHosts	Lists the hosts running the Directory server. The C API uses this key.
ldapSizeLimit +	Specifies the maximum number of entries returned from a search operation when the Directory server is being used with less than root privileges.
ldapTimeLimit +	Sets a time limit, in seconds, on Directory Cache server search operations.
loginAliases	Specifies whether the system uses alias addresses, instead of the attribute <code>userLogin</code> , to authenticate users.
loginFilter	A list of <code>regex</code> substitution filters that are applied, in sequence, to every name supplied in a POP authentication query before the name is looked up in the Directory database.

Configuration Key Name	Description
masterSearchRoot	Specifies the base entry to be used for searches on the master server.
numLdapConnections +	Represents the number of connections maintained in the pool between the client and the Directory Cache server.
partition +	Defines a partition LDAP object. This object contains the definitions of the partitions in the 'partition' attribute. <code>imdircacheserv</code> or <code>imdirserv</code> use these definitions to assign the <code>partitionName</code> attribute to objects.
replAreaSpec	Defines replication area specifications by referring to partition and attribute selection definitions. The names assigned to replication area specifications are referred to in the <code>replArea</code> attribute of a replication agreement.
rootBindAccess +	Determines whether you can log in and authenticate if you do not log in as <code>root</code> .
updateThreadRetryPeriod	Specifies the retry interval after a failure occurs during an update.
/*/imdbcontrol/defaultDirServer +	Specifies the LDAP server (either the Directory server or the Directory Cache server) to which <code>imdbcontrol</code> connects if the host and port are not specified on the command line. This is an <code>imdbcontrol</code> key.

Statistics

Statistics files contain information that measures system performance. The Directory Cache server writes the following statistics in the table below to `imdircacheserv.stat`.

Event	Description
StatAccumulatedConnections	Total number of connections made to <code>imdircacheserv</code> .
StatAccumulatedReadThrus	Number of read-through requests to <code>imdirserv</code> and the Directory database.

Event	Description
StatAuthReadThrus	Number of read-through requests to imdirserv and the Directory database in which authentication succeeded.
StatBadPasswordReturns	Number of validation requests, including read-throughs and authoritative cache lookups, that returned the error BAD PASSWORD, meaning that the input password or SMTP address was incorrect.
StatBytesSent	Number of bytes sent to imdirserv.
StatCachedItemLocks	Number of items currently locked in the entry cache of imdircacheserv. This is the number of items in use.
StatCachedItems	Number of items stored in the entry cache of imdircacheserv.
StatCachedItemSize	Total size, in bytes, of the items cached in the entry cache of imdircacheserv.
StatConnections	Number of current connections.
StatCosCacheItemLocks	Number of items currently locked in the class-of-service constraint cache. This is the number of items in use.
StatCosCacheItems	Number of class-of-service constraint sets kept in the Directory Cache database.
StatCosCacheItemSize	Total size of the class-of-service constraint cache in bytes.
StatEntriesSent	Number of data entries sent to the client.
StatFailedConnections	Number of failed connections. Connections fail when an attempt to create a socket for the client fails, typically because it has reached the maximum number of connections.
StatFailedSearches	Number of search requests that failed due to an error (not because the information was not there).
StatInactiveReturns	Number of requests that returned an account status of Deleted, Suspended, Locked, or Maintenance.
StatLookupFailedReturns	Number of validation requests in which lookup fails.
StatOKPasswordReturns	Number of validation requests that returned a successful lookup.
StatOpsCompleted	Number of operations (read-throughs and write-throughs) completed successfully by imdircacheserv.

Event	Description
StatOpsInitiated	Number of operations (read-throughs and write-throughs) requested by imdircacheserv.
StatQueriesFailed	Number of queries that failed due to unknown status or to a problem generating a class-of-service. <i>Note: StatInactiveReturns, StatBadPassword, and StatLookupFailed are not included here.</i>
StatQueriesProcessed	Number of queries processed.
StatQueriesSucceeded	Number of queries that succeeded.
StatReadThrusFailed	Number of read-throughs to imdirserv that failed.
StatRecentUpdates	Number of updates from the Directory database.
StatUnknownUserReturns	Number of user validation requests that returned the error UNKNOWN USER.
StatUpdateTime	Number of seconds spent processing updates from the Directory database.
StatWriteOperations	Number of write operations requested, including add, delete, and modify operations.
StatWritesFailed	Number of failed write-throughs to the Directory server.
StatWritesProcessed	Number of write-throughs processed to the Directory server.
StatWritesSucceeded	Number of successful write-throughs to the Directory server.
StatWritesUnknownUser	Number of write-through requests that returned the error UNKNOWN USER.

4

Replicating and Partitioning Data

This chapter discusses the concepts of replication and partitioning and provides procedures for replicating data at your site.

This chapter covers:

- Overview of replication and partitioning
- Planning your replication design
- Defining a replication agreement
- Setting up a replication agreement
- Examples of replication agreements

Overview of Replication and Partitioning

This section explains the concepts of replication and partitioning.

Replication

Replication is the process by which directory data is copied from the Directory server to one or more Directory Cache servers, which can be located on different host machines. An InterMail Mx system typically includes at least two Directory Cache servers.

A replica set is a set of identical Directory Cache servers that are interchangeable for satisfying client requests because they contain the same directory data. A replica set is specified as a list of host names. A client first tries to communicate with the Directory Cache server on the first host on the list. If that host is unavailable, it tries the other hosts in order. All clients can use the same replica set, or you can define multiple replica sets, where each replica set contains a portion of the data (see “Partitioning” on page 36). Using replica sets enables you to:

- Spread the request load across several host machines
- Store Directory information locally for local requesting clients

- Ensure continuous operation if one server or host machine fails

Figure 4 illustrates the concept of a replica set.

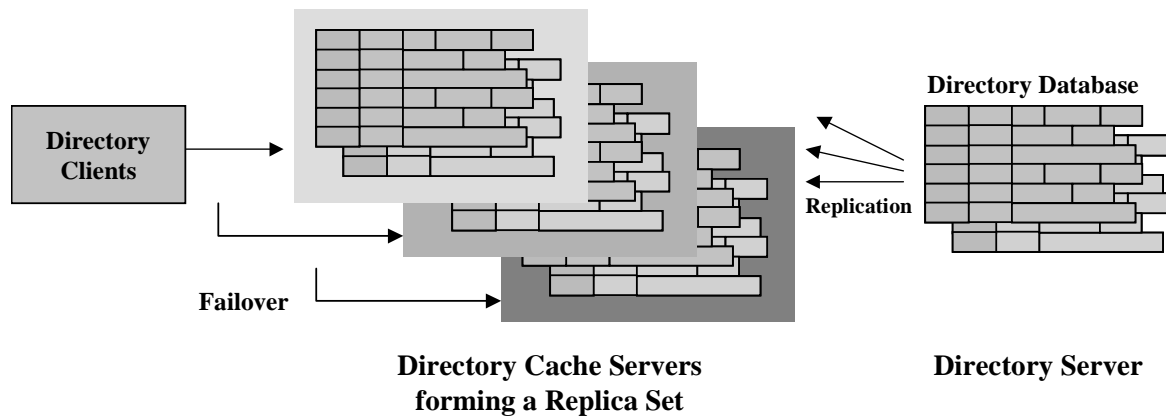


Figure 4 Replica set

You specify a replica set using the `ldapServerHosts` and `dirRmeHosts` configuration keys for the LDAP and RME protocols, respectively. These keys are described in Chapter 8.

Partitioning

Directory information can be divided, or partitioned, among different Directory Cache servers residing on different hosts. There are two basic types of partitioning:

- Application partitioning, which separates different directory applications across different Directory Cache servers. For example, one Directory Cache server could be dedicated to mail delivery, while another could be dedicated to looking up and updating white-page information such as names and addresses. Each of these Directory Cache servers could then be replicated (copied) for load balancing and failover capability.
- Object partitioning, which is used to increase system scalability and to enable the directory to hold more data without overwhelming one host machine. In this scheme, database entries belong to one partition only. For example, Directory data could be partitioned by:
 - Geographic location
 - Organization
 - Function
 - Protocol

Note: You can combine application and object partitioning by splitting the directory into two application-based partitions, and further splitting each of these by site or other partitioning criterion of your choice.

Planning your Replication Design

You design the replication and partitioning scheme for your site based on:

- Client data needs
- System utilization
- Quality-of-service requirements of each client application

The following table shows the impact of client data needs, system utilization, and quality-of-service requirements on the replication design for three different types of Integrated Service Directory (ISD) clients:

- End-user address book e-mail clients, which perform LDAP queries for white-page information
- InterMail servers, which perform RME queries for e-mail-related account information
- InterManager clients, used by administrators to maintain directory information with LDAP

Replication Design Basis	Client Data Needs	System Utilization	Quality-of-Service Requirements	Resulting Replication Design
End-user address book clients	<ul style="list-style-type: none"> • Account entries only • Small set of attributes 	<ul style="list-style-type: none"> • Moderate load • Range of queries • Read only 	<ul style="list-style-type: none"> • Low-availability requirements • Moderate response times 	<ul style="list-style-type: none"> • Regional partitioning • One Directory Cache server per partition • Only white-page data is replicated.
InterMail servers	<ul style="list-style-type: none"> • Account and domain entries • Most attributes 	<ul style="list-style-type: none"> • Heavy load • Simple queries • Read only 	<ul style="list-style-type: none"> • High-availability requirements • Fast response times 	<ul style="list-style-type: none"> • Partitioning based on mailbox ID • Three Directory servers per replica set • All account and domain data is replicated.
InterManager clients	<ul style="list-style-type: none"> • All directory entries • All attributes 	<ul style="list-style-type: none"> • Light load • Complex queries • Reads and writes 	<ul style="list-style-type: none"> • Moderate-availability requirements • Slow response times 	<ul style="list-style-type: none"> • No partitioning • Two Directory servers per replica set • All data is replicated.

Figure 5 illustrates replication designs for these three types of Directory clients, all in use within a single InterMail installation.

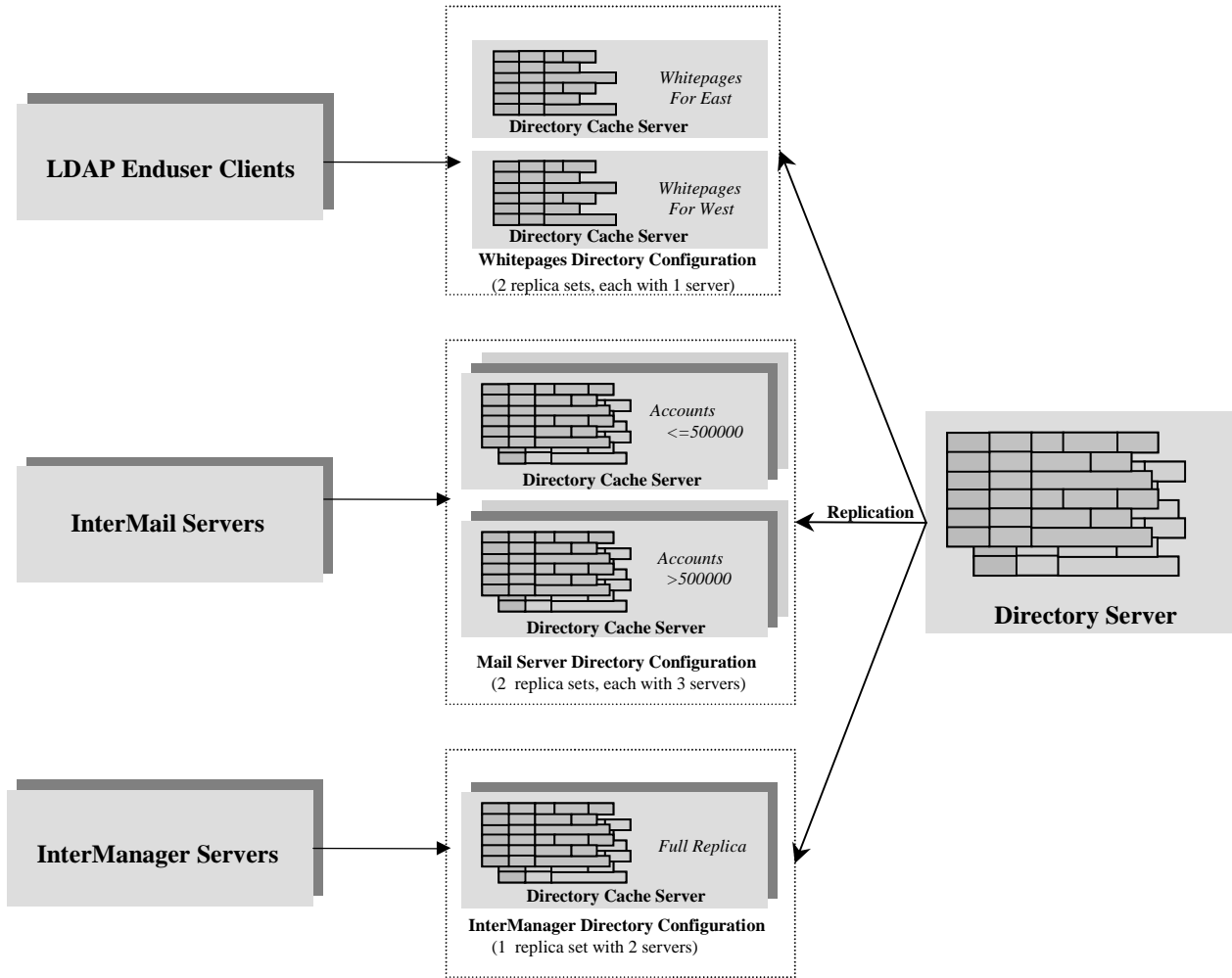


Figure 5 Replication designs for three types of Directory clients

Defining a Replication Agreement

A replication agreement is the vehicle used to partition and replicate directory data among different Directory Cache servers. The agreement is established between a supplier server, which supplies the information to be replicated, and a consumer server, which is the destination for the replicated data. In InterMail, the supplier is the Directory server and the consumer is a Directory Cache server.

The replication agreement specifies which Directory database entries are copied to and maintained by a particular Directory Cache server. Each Directory Cache server uses its replication agreement as a “filter” when retrieving updates from the Directory

server change log, storing only those entries that match the replication agreement. Entries that match a filter specification are directed to a particular Directory Cache database while being “filtered out” of the others.

Replication agreements also specify:

- Attributes to be replicated to the consumer server
- Supplier server hostname and LDAP port number
- Update interval, in seconds
- Identity and password the consumer server uses to connect to the supplier server to receive updates

Storage of Replication Agreements

Replication agreements are defined in the Configuration database and then loaded and stored as LDAP entries in the Directory Cache database. You use the `imdirsync` utility to copy these agreements from the Configuration database to the Directory Cache database. For more information on directory management utilities, see Chapter 9.

Whenever you modify a replication agreement, you must run the `imdirsync` utility. If you do not, you will receive a warning that the replication agreements in the Configuration database and the Directory Cache database do not match, and data replication will not work properly.

To modify a replication agreement:

1. Shut down the Directory server and the Directory Cache server, using the `imctrl` administrative command. For the syntax of this command, see the *InterMail Mx Reference Guide*.
2. Modify the replication agreement by modifying the appropriate configuration keys. For more information, see “Configuration Keys Used for Replication Agreements” on page 42.
3. Run `imdirsync` to copy the new replication agreement to the Directory Cache database.
4. Restart the Directory server and the Directory Cache server using the `imctrl` command.

Chaining Directory Cache Servers

Ideally, you define replication agreements so that a single Directory Cache server can satisfy each client query. In some cases, however, this may not be possible. For example, to improve scalability, you might create a replication design in which each Directory Cache database holds a portion of the data and routes information for the rest of the data. In such a case, the Directory Cache server answers some requests locally, uses the routing list information to contact the other Directory Cache servers for requests that require access to the data on those servers, and returns the combined

results to the client after the other servers in the chain have completed their searches. This process is known as chaining.

You use the `chainingInfo` configuration key to specify the chaining sequence. To do this, you provide the following information:

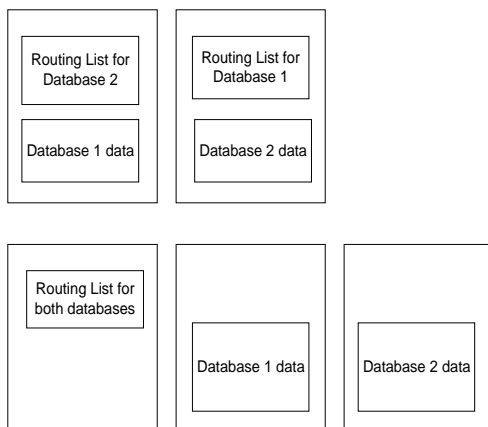
- Name of the host of the first Directory Cache server to be contacted by an RME client server to respond to a query
- Name of the set of Directory database entries to be mapped to a host in the chain
- Names of the host machines in the chain in the order they are contacted

For detailed information on this key, see Chapter 8.

Note: Chaining can be used only for RME queries, such as those made by the POP, IMAP, Message Transport Agent (MTA), and Message Store (MSS) servers. LDAP queries, such as those made by Web servers, are answered by the Directory Cache server receiving the request.

Chaining Scenarios Involving Routing Lists

When you partition data, you can dedicate one Directory Cache server solely to chaining, so it acts as a router to the Directory Cache server controlling the attributes you are searching for. Alternatively, each Directory Cache server can control all of the attributes for a portion of the data, holding only the routing attributes for the data partitioned to other Directory Cache servers. For example, a Directory Cache server could control all data accessed by POP servers, as well as indexed attributes for data controlled by other Directory Cache servers. Figure 6 illustrates these alternatives.



Two Directory Cache servers, each controlling a routing list of the data stored in the other's Directory Cache database.

Three Directory cache servers, one containing a routing list only, the others containing data only.

Figure 6 Sample chaining configurations

Configuration Keys Used for Replication Agreements

The filters used to partition data are defined and stored within the Configuration database on all Directory Cache server host machines. The configuration key `ldapReplicationAgreement` defines the partitions to be used for a particular host machine. It also references several other configuration keys to define the filters to be used for a particular Directory Cache server host machine. These keys are:

- `attributeSelection`
- `partition`
- `replAreaSpec`

Each of these configuration keys is described briefly below. For detailed information on these Directory Cache server configuration keys, see Chapter 8.

ldapReplicationAgreement

The `ldapReplicationAgreement` key defines an LDAP entry describing the complete replication agreement between one or more Directory Cache servers and the Directory server. The `attributeSelection`, `partition`, and `replAreaSpec` configuration keys enable you to define a replication area once, and then refer to it in replication agreements for all Directory Cache servers in a replica set.

Note: You can have only one replication agreement per Directory Cache server.

attributeSelection

You use the `attributeSelection` key to select the set of attributes for each partition, assign a name to the partition, and specify whether those attributes are to be filtered into or out of the replicated entries. An attribute set definition can be used by any Directory Cache server.

partition

You use the `partition` key to define the selection criteria for entries in the Directory Information Tree (DIT) to be included in each partition. A partition definition can be used by any Directory Cache server.

replAreaSpec

You use the `replAreaSpec` key to label the set of attributes and entries to be copied to the consumer server. You specify the replication area by referring to an attribute selection name and a partition name. A replication area definition can be used by any Directory Cache server.

Setting Up a Replication Agreement

Figure 7 illustrates, and the following text describes, the steps involved in creating a replication agreement. The numbered list in the text corresponds to the steps in the figure.

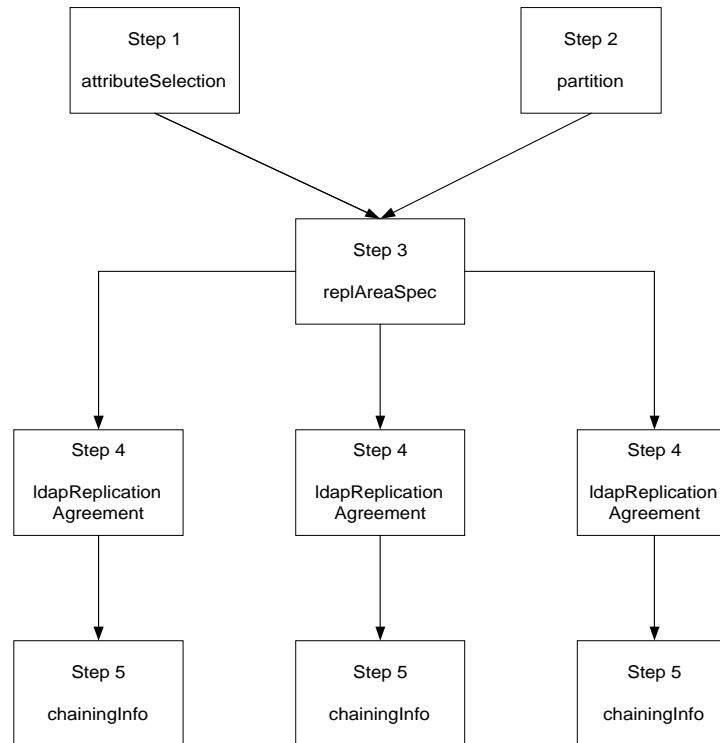


Figure 7 Creating replication agreements

Figure 7 depicts the steps you follow to create a replication agreement:

1. Use the `attributeSelection` configuration key to:
 - a. Choose the attributes you want to group.
 - b. Name the group.

Note: The name of the attribute group is referenced as the replication agreement name in the `ldapReplicationAgreement` configuration key.

- c. Specify whether the group is used to filter the grouped attributes into or out of the replicated entries.
2. Use the `partition` configuration key to define the partition name and the selection criteria for entries to include in each partition.

3. Use the `replAreaSpec` configuration key to specify the attribute group names and the partition names you want to include in each replication area.
4. Use the `ldapReplicationAgreement` configuration key to assign replication areas to the Directory Cache server.
5. Use the `chainingInfo` configuration key to specify which host machine should be contacted for queries about a particular entry.

Note: For load balancing purposes, you can use the `dirRmeHosts` configuration key to assign a particular Directory Cache server to an RME client, such as a POP, IMAP, MTA, or MSS server. To assign a particular Directory Cache server to an LDAP client, such as WebEdge, InterManager, or the InterMail APIs, use the `ldapServerHosts` configuration key. For detailed information on these Directory configuration keys, see Chapter 8.

Examples of Replication Agreements

This section provides examples of some of the ways replication agreements can be created for an InterMail Mx installation. It covers the following scenarios, in increasing order of complexity:

- Replicating the entire Directory database, in which one Directory Cache database contains a complete copy of the Directory database
- Using a replica set, in which each Directory Cache server has the same replication agreement
- Using chaining, in which one Directory Cache server holds index information only
- Using partitioning, in which directory data is partitioned among several Directory Cache servers using several replication agreements
- Using replica sets with partitions, in which directory data is partitioned and each partition is replicated.
- Using application partitioning, in which directory data is partitioned by application.

Replicating a Complete Copy of the Directory Database

In this example, there is only one Directory Cache database, and it contains a complete copy of the Directory database. The Directory Cache server is running on a host named `Host1`, and the update interval is 60 seconds. Figure 8 depicts this configuration.

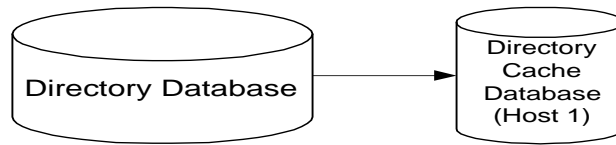


Figure 8 Replicating a complete copy of the directory database

This example illustrates the default replication agreement for a new installation. Because a replication area is not defined, all entries are replicated.

To define the replication agreement:

1. Specify your attribute selection criteria.

The Directory Cache database holds a complete replica of all the data in the Directory database. Therefore, you do not use the `attributeSelection` configuration key.

2. Define your partitions.

The Directory Cache server copies the entire Directory database into its Directory Cache database. Therefore, you do not use the `partition` configuration key.

3. Specify your replication area.

All objects and attributes in the Directory database are to be copied to the Directory Cache server. Therefore, you do not use the `replAreaSpec` configuration key.

4. Set up your replication agreement.

The replication agreement indicates that all entries are to be copied from the Directory server to the Directory Cache server on `Host1` with an update interval of 60 seconds. You set up the replication agreement using the `ldapReplicationAgreement` configuration key, as follows:

```
/Host1/imdircachserv/ldapReplicationAgreement:  
[cn: defaultReplicationAgreement]  
[updateInterval: 60]
```

5. Set up your chaining configuration.

Chaining is not used in this example.

Using a Replica Set

In this example, a replica set is used, meaning that each Directory Cache database contains identical entries and each Directory Cache server has the same replication agreement (Figure 9). This configuration increases the availability of the Integrated Services Directory (ISD) by supporting Directory Cache server failover. Only the attributes used by the MTA and MSS servers are replicated in this example.

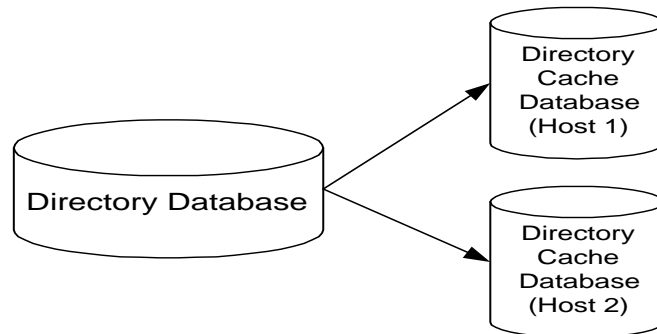


Figure 9 Using a replica set

The `dirRmeHosts` configuration key specifies which host each client should contact first, as well as a backup host, in order to distribute the load evenly across Directory Cache servers. In this example, you have two client MTA servers, `ClientA` and `ClientB`. The `dirRmeHosts` key is set as follows:

```

/ClientA/MTA/dirRmeHosts: Host1, Host2
/ClientB/MTA/dirRmeHosts: Host2, Host1
  
```

With this setting, one MTA client contacts `Host1` first. If `Host1` is not available, it contacts `Host2`. The other MTA client contacts `Host2` first. If `Host2` is not available, it contacts `Host1`.

To define the replication agreement:

1. Specify your attribute selection criteria.

Use the `attributeSelection` configuration key to specify the attributes for this group. Define `MTA_MSS_ATTRS` as the name of the group that selects the attributes required for the MTA and MSS servers:

```

/*imdircacheserv/attributeSelection:
[MTA_MSS_ATTRS :: include (objectClass $ mailAlternateAddress $
mailAutoReplyHost $mailForwardingAddress $mailSmtRelayHost $
mailForwarding $ mailDeliveryOption $ mailAutoReplyMode $
mailMtaFilter $ mailSmtAuth $ mailSmtAccess $ mailSmtSslAccess $
mailQuotaBounceNotify $ mailBoxId $ mailBoxStatus $
mailMessageStore $ mailQuotaTotKB $ mailQuotaMaxMsgKB $
mailQuotaMaxMsgs $ mailQuotaThreshold)]
  
```

Note: `/*/` indicates that this attribute selection applies to all Directory Cache server host machines.

2. Define your partition.

Use the `partition` configuration key to define the partition:

```
/*/common/partition:
[Name:allObjects BASE:root FILTER:(objectClass=*)]
```

3. Specify your replication area.

Use the `replAreaSpec` configuration key to construct the replication area from the attribute group defined in step 1:

```
/*/imdircacheserv/replAreaSpec:
[MTA_MSS :: PARTITION:allObjects ATTR_SEL: MTA_MSS_ATTRS]
```

4. Set up your replication agreement.

Use the `ldapReplicationAgreement` configuration key to identify the data that the Directory Cache servers running on `Host1` and `Host2` are to copy from the Directory server:

```
/Host1/imdircacheserv/ldapReplicationAgreement:
[cn: RepSet]
[updateInterval: 60]
[replArea: MTA_MSS]
/Host2/imdircacheserv/ldapReplicationAgreement:
[cn: RepSet]
[updateInterval: 60]
[replArea: MTA_MSS]
```

5. Set up your chaining configuration.

Chaining is not used in this example.

Using Chaining

In this example, one Directory Cache server functions as a router server, controlling only chaining information. The other Directory Cache servers control only data. The chaining process routes the data from the router server to other Directory Cache servers.

The router server is the primary server that clients will contact. It holds chaining information for every object in the Directory database, and chains requests to the Directory Cache servers that hold the requested data. Assume that this server is running on host `HostRouter`. Figure 10 depicts this configuration.

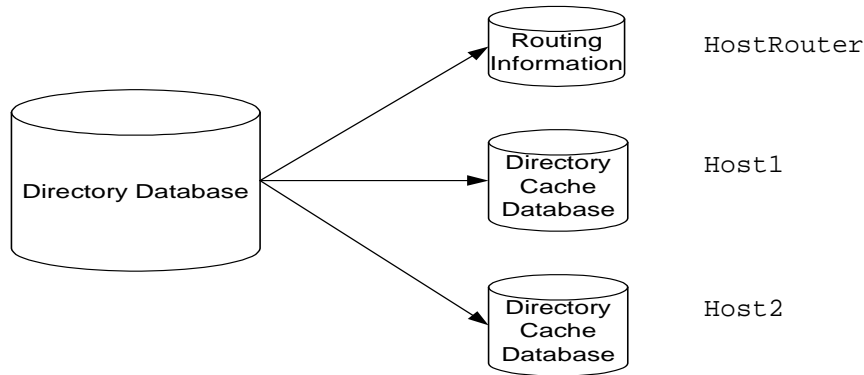


Figure 10 Using chaining

The `dirRmeHosts` configuration key specifies which host each client should contact first, as well as a backup host, in order to distribute the load evenly across Directory Cache servers. In this example, you have two client MTA servers, `ClientA` and `ClientB`. The `dirRmeHosts` key is set as follows:

```

/ClientA/MTA/dirRmeHosts: HostRouter
/ClientB/MTA/dirRmeHosts: HostRouter
  
```

With this setting, all MTA clients contact the router server first. The router server then chains each request to either `Host1` or `Host2`, depending on which one contains the data being sought.

To define the replication agreement:

1. Specify your attribute selection criteria.

In this example, you define three different attribute selection criteria:

- `MTA_MSS_ATTRS` is the name of the group that selects the attributes required for MTA and MSS servers.
- `MTA_MSS_ROUTER_ATTRS` is the name of the group that selects the attributes for the routing of account information. This kind of group is useful when a server contains routing information for all accounts, yet holds only a subset of accounts or no account data at all.
- `NON_LEAF_ATTRS` is the name of the group that selects the attributes for the non-leaf objects. Non-leaf objects are directory entries that have child entries below them in the Directory Information Tree (DIT) hierarchy. The non-leaf objects must be replicated in order for any leaf objects below them to be replicated.

Use the `attributeSelection` configuration key to define the attribute selection criteria as follows:

```

/*imdircacheserv/attributeSelection:
[MTA_MSS_ATTRS :: include (objectClass $ mailAlternateAddress $
mailAutoReplyHost $mailForwardingAddress $mailSmtRelayHost $
mailForwarding $ mailDeliveryOption $ mailAutoReplyMode $
  
```

```

mailMtaFilter $ mailSmtpAuth $ mailSmtpAccess $ mailSmtpSslAccess $
mailQuotaBounceNotify $ mailBoxId $ mailBoxStatus $
mailMessageStore $ mailQuotaTotKB $ mailQuotaMaxMsgKB $
mailQuotaMaxMsgs $ mailQuotaThreshold))
[MTA_MSS_ROUTER_ATTRS :: include (objectClass $
mailAlternateAddress $ mailForwardingAddress $ mailBoxId)]
[NON_LEAF_ATTRS :: include (objectClass)]

```

2. Define your partitions.

In this example, you define three partitions:

- low contains accounts with a mailBoxID value of less than or equal to 500,000.
- high contains accounts with a mailBoxId value of greater than 500,000.
- non-leaf defines a partition to replicate non-leaf objects, meaning directory entries that have child entries below them in the DIT. Non-leaf entries must be replicated in order to successfully replicate their child entries.

Note: This configuration represents a growing organization that has added so many new mailboxes that another Directory Cache server is needed to relieve the load. All new entries, identified by a mailBoxId value greater than 500,000, are handled by the second Directory Cache server.

Use the partition configuration key to define the partitions:

```

/*/common/partition:
[Name:low BASE:dc=com FILTER:(mailBoxId <= 500000)]
[Name:high BASE: dc=com FILTER: (mailBoxId > 500000)]
[Name:non-leaf BASE:root
FILTER:(|(objectclass=domain)(objectclass=realms)
(objectclass=dcObject) (objectClass=organization)
(objectclass=organizationalUnit))]

```

3. Specify your replication areas.

Use the replAreaSpec configuration key to construct replication areas from the attribute groups and partitions you just defined:

```

/*/imdircacheserv/replAreaSpec:
[MTA_MSS_LOW :: PARTITION: low ATTR_SEL: MTA_MSS_ATTRS]
[MTA_MSS_HIGH :: PARTITION: high ATTR_SEL: MTA_MSS_ATTRS]
[MTA_MSS_LOW_ROUTER :: PARTITION: low
ATTR_SEL:MTA_MSS_ROUTER_ATTRS]
[MTA_MSS_HIGH_ROUTER ::PARTITION: high ATTR_SEL:
MTA_MSS_ROUTER_ATTRS]
[NON_LEAF :: PARTITION: non-leaf ATTR_SEL: NON_LEAF_ATTRS]

```

4. Set up your replication agreements.

Use the `ldapReplicationAgreement` configuration key to identify the data that the router server is to copy from the Directory server:

```
/HostRouter/imdircachesserv/ldapReplicationAgreement:  
[cn: Router]  
[updateInterval: 60]  
[replArea: MTA_MSS_LOW_ROUTER]  
[replArea: MTA_MSS_HIGH_ROUTER]  
/Host1/imdircachesserv/ldapReplicationAgreement:  
[cn: RALow]  
[updateInterval: 60]  
[replArea: MTA_MSS_LOW]  
[replArea: MTA_MSS_NON_LEAF]  
/Host2/imdircachesserv/ldapReplicationAgreement:  
[cn: RAHigh]  
[updateInterval: 60]  
[replArea: MTA_MSS_HIGH]  
[replArea: MTA_MSS_NON_LEAF]
```

5. Set up your chaining configuration.

The router server uses the `chainingInfo` configuration key to contact another Directory Cache server to answer a request. Set the `chainingInfo` key as follows:

```
/*/imdircachesserv/chainingInfo:  
[MTA_MSS_LOW_ROUTER : Host1]  
[MTA_MSS_HIGH_ROUTER : Host2]
```

When the Directory Cache server on `HostRouter` encounters an object that has a `partitionName` value of `low`, the Directory Cache server maps the `partitionName` value to one of its replication area names, in this case `MTA_MSS_LOW_ROUTER`. It uses this name to find the list of Directory Cache server hosts serving the corresponding replication area specification (`MTA_MSS_LOW`) and then queries one of these hosts depending on availability. In this example, there is only one host, `Host1`.

Similarly, the `HostRouter` Directory Cache server contacts the Directory Cache server on `Host2` for objects whose `partitionName` attribute value is `high`.

Using Partitioning with Multiple Replication Agreements

In this example, routing information and the data itself are both stored on each of the servers in each partition. One Directory Cache server, running on `Host1`, holds all the data for objects in partition `low` and all routing information for data in partition `high`. The other Directory Cache server, running on `Host2`, holds all the data for objects in partition `high` and all routing information for data in partition `low`. Figure 11 depicts this configuration.

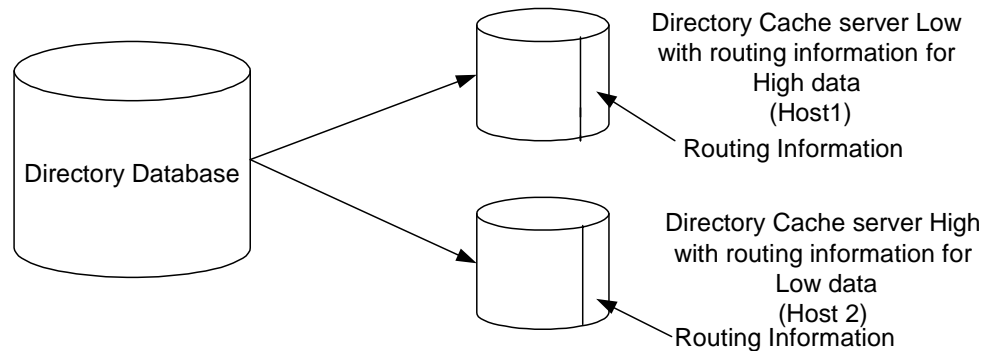


Figure 11 Using partitioning with multiple replication agreements

The `dirRmeHosts` configuration key specifies which host each client should contact first, as well as a backup host, in order to distribute the load evenly across Directory Cache servers. In this example, you have two client MTA servers, `ClientA` and `ClientB`. The `dirRmeHosts` key is set as follows:

```
/ClientA/MTA/dirRmeHosts: Host1, Host2
/ClientB/MTA/dirRmeHosts: Host2, Host1
```

With this setting, one MTA client contacts `Host1` first. If `Host1` is not available, it contacts `Host2`. The other MTA client contacts `Host2` first. If `Host2` is not available, it contacts `Host1`.

To define the replication agreement:

1. Specify your attribute selection criteria.

In this example, you define three different attribute selection criteria:

- `MTA_MSS_ATTRS` is the name of the group that selects the attributes required for MTA and MSS servers.
- `MTA_MSS_ROUTER_ATTRS` is the name of the group that selects the attributes for the routing of account information. This kind of group is useful when a server contains routing information for all accounts, yet holds only a subset of accounts or no account data at all.
- `NON_LEAF_ATTRS` is the name of the group that selects the attributes for the non-leaf objects. Non-leaf objects are directory entries that have child entries below them in the Directory Information Tree (DIT) hierarchy. The non-leaf objects must be replicated in order for any leaf objects below them to be replicated.

Use the `attributeSelection` configuration key to define the attribute selection criteria as follows:

```
/*/imdircacheserv/attributeSelection:
[MTA_MSS_ATTRS :: include (objectClass $ mailAlternateAddress $
mailAutoReplyHost $ mailForwardingAddress $ mailSmtRelayHost $
mailForwarding $ mailDeliveryOption $ mailAutoReplyMode $
mailMtaFilter $ mailSmtAuth $ mailSmtAccess $ mailSmtSslAccess $
mailQuotaBounceNotify $ mailBoxId $ mailBoxStatus $
mailMessageStore $ mailQuotaTotKB $ mailQuotaMaxMsgKB $
mailQuotaMaxMsgs $ mailQuotaThreshold)]
[MTA_MSS_ROUTER_ATTRS :: include (objectClass $
mailAlternateAddress $ mailForwardingAddress $ mailBoxId)]
[NON_LEAF_ATTRS :: include (objectClass)]
```

Note: `/*/` indicates that this attribute selection applies to all Directory Cache server host machines.

2. Define your partitions.

In this example, you define three partitions:

- `low` contains accounts with a `mailBoxId` value of less than or equal to 500,000.
- `high` contains accounts with a `mailBoxId` value of greater than 500,000.
- `non-leaf` defines a partition to replicate non-leaf objects, meaning directory entries that have child entries below them in the DIT. Non-leaf entries must be replicated in order to successfully replicate their child entries.

Note: This configuration represents a growing organization that has added so many new mailboxes that another Directory Cache server is needed to relieve the load. All new entries, identified by a `mailBoxId` value greater than 500,000, are handled by the second Directory Cache server.

Use the `partition` configuration key to define the partitions:

```
/*/common/partition:
[Name:low BASE:dc=com FILTER:(mailBoxId <= 500000)]
[Name:high BASE: dc=com FILTER: (mailBoxId > 500000)]
[Name:non-leaf BASE:root
FILTER:(|(objectclass=domain)(objectclass=realms)
(objectclass=dcObject) (objectClass=organization)
(objectclass=organizationalUnit))]
```

3. Specify your replication areas.

Use the `replAreaSpec` configuration key to construct replication areas from the attribute groups and partitions you just defined:

```

/*/imdircacheserv/replAreaSpec:
[MTA_MSS_LOW :: PARTITION: low ATTR_SEL: MTA_MSS_ATTRS]
[MTA_MSS_HIGH :: PARTITION: high ATTR_SEL: MTA_MSS_ATTRS]
[MTA_MSS_LOW_ROUTER :: PARTITION: low
ATTR_SEL:MTA_MSS_ROUTER_ATTRS]
[MTA_MSS_HIGH_ROUTER ::PARTITION: high ATTR_SEL:
MTA_MSS_ROUTER_ATTRS]
[NON_LEAF :: PARTITION: non-leaf ATTR_SEL: NON_LEAF_ATTRS]

```

4. Set up your replication agreements.

Use the `ldapReplicationAgreement` configuration key to identify the data that the Directory Cache servers running on `Host1` and `Host2` are to copy from the Directory server:

```

/Host1/imdircacheserv/ldapReplicationAgreement:
[cn: RALowRouteForHigh]
[updateInterval: 60]
[replArea: MTA_MSS_LOW]
[replArea: MTA_MSS_HIGH_ROUTER]
[replArea: NON_LEAF]

/Host2/imdircacheserv/ldapReplicationAgreement:
[cn: RAHighRouteForLow]
[updateInterval: 60]
[replArea: MTA_MSS_HIGH]
[replArea: MTA_MSS_LOW_ROUTER]
[replArea: NON_LEAF]

```

5. Set up your chaining configuration.

Set the `chainingInfo` key as follows:

```

/Host1/imdircacheserv/chainingInfo:
[MTA_MSS_HIGH_ROUTER: Host2]
/Host2/imdircacheserv/chainingInfo:
[MTA_MSS_LOW_ROUTER: Host1]

```

Using Replica Sets with Partitions

In this example, directory data is partitioned and each partition is replicated. Such a configuration combines the benefits of scalability and availability by using both replication and partitioning. Figure 12 depicts this configuration.

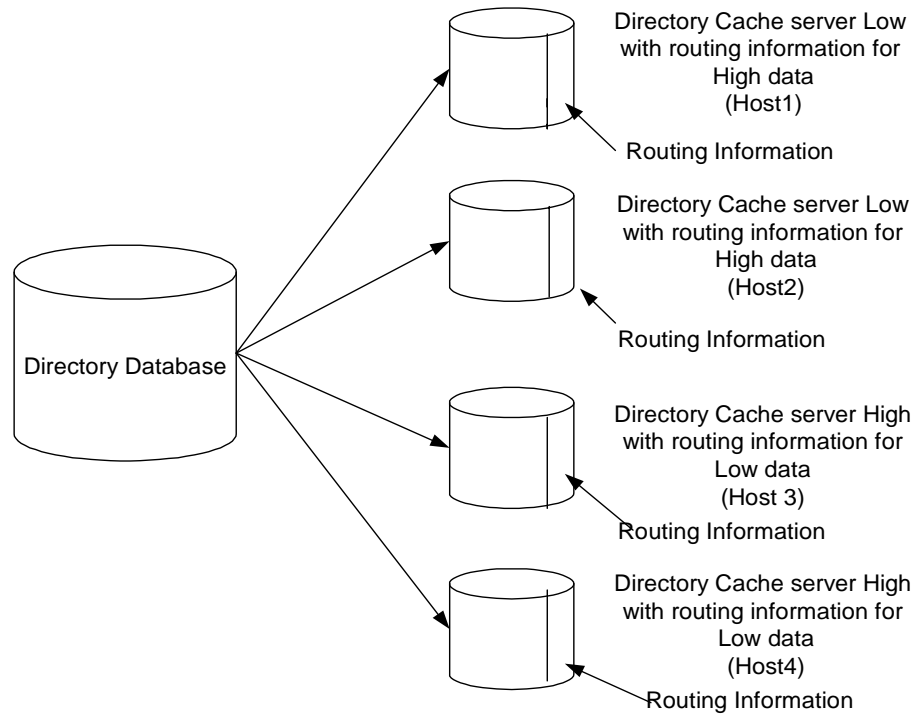


Figure 12 Using replica sets with partitions

The `dirRmeHosts` configuration key specifies which host each client should contact first, as well as a backup host, in order to distribute the load evenly across Directory Cache servers. In this example, you have four client MTA servers, `ClientA`, `ClientB`, `ClientC`, and `ClientD`.

```
/ClientA/MTA/dirRmeHosts: Host1, Host2, Host3, Host4
/ClientB/MTA/dirRmeHosts: Host2, Host3, Host4, Host1
/ClientC/MTA/dirRmeHosts: Host3, Host4, Host1, Host2
/ClientD/MTA/dirRmeHosts: Host4, Host1, Host2, Host3
```

With this setting, one fourth of the MTA clients contact `Host1` first. If `Host1` is not available, they contact `Host2`. If `Host2` is not available, they contact `Host3`, and so on. One fourth of the MTA clients contact `Host2` first. If `Host2` is not available, they contact `Host3`. One fourth of the MTA clients contact `Host3` first, and one fourth of the MTA clients contact `Host4` first.

To define the replication agreement:

1. Specify your attribute selection criteria.

In this example, you define three different attribute selection criteria:

- `MTA_MSS_ATTRS` is the name of the group that selects the attributes required for MTA and MSS servers.

- MTA_MSS_ROUTER_ATTRS is the name of the group that selects the attributes for the routing of account information. This kind of group is useful when a server contains routing information for all accounts, yet holds only a subset of accounts or no account data at all.
- NON_LEAF_ATTRS is the name of the group that selects the attributes for the non-leaf objects. Non-leaf objects are directory entries that have child entries below them in the Directory Information Tree (DIT) hierarchy. The non-leaf objects must be replicated in order for any leaf objects below them to be replicated.

Use the `attributeSelection` configuration key to define the attribute selection criteria as follows:

```

/*/imdircachesserv/attributeSelection:
[MTA_MSS_ATTRS :: include (objectClass $ mailAlternateAddress $
mailAutoReplyHost $ mailForwardingAddress $ mailSmtpRelayHost $
mailForwarding $ mailDeliveryOption $ mailAutoReplyMode $
mailMtaFilter $ mailSmtpAuth $ mailSmtpAccess $ mailSmtpSslAccess $
mailQuotaBounceNotify $ mailBoxId $ mailBoxStatus $
mailMessageStore $ mailQuotaTotKB $ mailQuotaMaxMsgKB $
mailQuotaMaxMsgs $ mailQuotaThreshold)]
[MTA_MSS_ROUTER_ATTRS :: include (objectClass $
mailAlternateAddress $ mailForwardingAddress $ mailBoxId)]
[NON_LEAF_ATTRS :: include (objectClass)]

```

Note: `/*/` indicates that this attribute selection applies to all Directory Cache server host machines.

2. Define your partitions.

In this example, you define three partitions:

- `low` contains accounts with a `mailBoxId` value of less than or equal to 500,000.
- `high` contains accounts with a `mailBoxId` value of greater than 500,000.
- `non-leaf` defines a partition to replicate non-leaf objects, meaning directory entries that have child entries below them in the DIT. Non-leaf entries must be replicated in order to successfully replicate their child entries.

Note: This configuration represents a growing organization that has added so many new mailboxes that another Directory Cache server is needed to relieve the load. All new entries, identified by a `mailBoxId` value greater than 500,000, are handled by the second Directory Cache server.

Use the `partition` configuration key to define the partitions:

```

/*/common/partition:
[Name:low BASE:dc=com FILTER:(mailBoxId <= 500000)]
[Name:high BASE: dc=com FILTER: (mailBoxId > 500000)]
[Name:non-leaf BASE:root]

```

```
FILTER: (|(objectclass=domain)(objectclass=realms)
(objectclass=dcObject) (objectClass=organization)
(objectclass=organizationalUnit))]
```

3. Specify your replication areas.

Use the `replAreaSpec` configuration key to construct replication areas from the attribute groups and partitions you just defined:

```
/*/imdircachesserv/replAreaSpec:
[MTA_MSS_LOW :: PARTITION: low ATTR_SEL: MTA_MSS_ATTRS]
[MTA_MSS_HIGH :: PARTITION: high ATTR_SEL: MTA_MSS_ATTRS]
[MTA_MSS_LOW_ROUTER :: PARTITION: low
ATTR_SEL:MTA_MSS_ROUTER_ATTRS]
[MTA_MSS_HIGH_ROUTER ::PARTITION: high ATTR_SEL:
MTA_MSS_ROUTER_ATTRS]
[NON_LEAF :: PARTITION: non-leaf ATTR_SEL: NON_LEAF_ATTRS]
```

4. Set up your replication agreements.

Use the `ldapReplicationAgreement` configuration key to identify the data that data that the Directory Cache servers running on `Host1`, `Host2`, `Host 3`, and `Host4` are to copy from the Directory server:

```
/Host1/imdircachesserv/ldapReplicationAgreement:
[cn: RALowRouteForHigh]
[updateInterval: 60]
[replArea: MTA_MSS_LOW]
[replArea: MTA_MSS_HIGH_ROUTER]
/Host2/imdircachesserv/ldapReplicationAgreement:
[cn: RALowRouteForHigh]
[updateInterval: 60]
[replArea: MTA_MSS_LOW]
[replArea: MTA_MSS_HIGH_ROUTER]
/Host3/imdircachesserv/ldapReplicationAgreement:
[cn: RAHighRouteForLow]
[updateInterval: 60]
[replArea: MTA_MSS_HIGH]
[replArea: MTA_MSS_LOW_ROUTER]
/Host4/imdircachesserv/ldapReplicationAgreement:
[cn: RAHighRouteForLow]
[updateInterval: 60]
[replArea: MTA_MSS_HIGH]
[replArea: MTA_MSS_LOW_ROUTER]
```

5. Set up your chaining configuration.

Set the `chainingInfo` configuration key as follows:

```
/Host1/imdircachesserv/chainingInfo:
[MTA_MSS_HIGH_ROUTER: Host3, Host4]
/Host2/imdircachesserv/chainingInfo:
[MTA_MSS_HIGH_ROUTER: Host4, Host3]
/Host3/imdircachesserv/chainingInfo:
[MTA_MSS_LOW_ROUTER: Host1, Host2]
/Host4/imdircachesserv/chainingInfo:
[MTA_MSS_LOW_ROUTER: Host2, Host1]
```

Using Application Partitioning

In the previous examples, accounts were partitioned based upon their mailbox ID numbers. This example illustrates application partitioning, in which mail retrieval (IMAP), mail retrieval (POP), and white-page (WP) information are partitioned on different Directory Cache servers.

Assume that the Directory Cache server controlling the IMAP data runs on host `imap`; the Directory Cache server controlling the POP data runs on host `hpop`; and the Directory Cache server controlling the white-page data runs on host `hwp`. Figure 13 depicts this configuration.

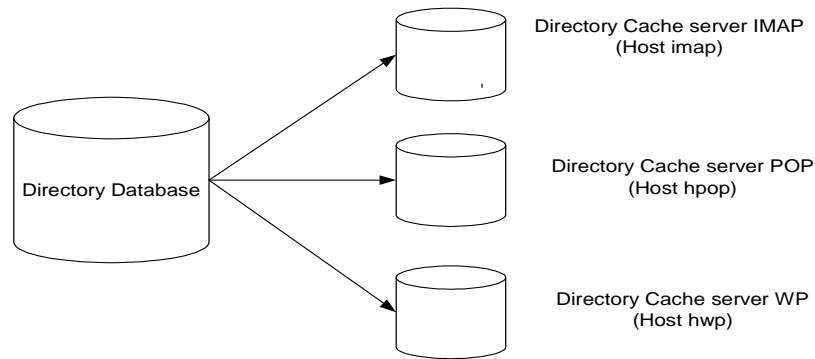


Figure 13 Using application partitioning

The `dirRmeHosts` configuration key specifies which host each client should contact first, as well as a backup host, in order to distribute the load evenly across Directory Cache servers. In this example, IMAP clients contact host `imap`, POP clients contact host `hpop`, and all other clients contact host `hwp`.

To define the replication agreement:

1. Specify your attribute selection criteria.

Use the `attributeSelection` configuration key to specify the attribute selection criteria for the three groups:

```

/*/imdircacheserv/attributeSelection:
[IMAP :: include (objectclass $ mailImapAccess $
mailImapSslAccess)]
[POP :: include (objectclass $ mailBoxId $ mailBoxStatus $
mailPassword $ mailPasswordType $ mailPopProxyHost $
mailPopAccess $ mailPopSslAccess)]
[WP :: include (objectclass $ cn $ sn $ givenName $ street $
l $ c $ mail $ telephoneNumber $ title $
facsimileTelephoneNumber $ description)]
  
```

2. Define your partitions.

The partition P1 includes all mail user accounts:

```

/*/common/partition:
[P1 :: Base: dc=com Filter: (objectclass=mailUser)]
  
```

3. Specify your replication areas.

Use the `replAreaSpec` configuration key to construct the replication areas for the three groups:

```
/*/imdircachesserv/replAreaSpec:  
[IMAP :: Partition: P1 ATTR_SEL: IMAP]  
[POP :: Partition: P1 ATTR_SEL: POP]  
[WP :: Partition: P1 ATTR_SEL: WP]
```

4. Set up your replication agreements.

Use the `ldapReplicationAgreement` configuration key to identify the data that the Directory Cache servers running on the three hosts are to copy from the Directory server:

```
/hmta/imdircachesserv/ldapReplicationAgreement:  
[cn: RAimap]  
[updateInterval: 60]  
[replArea: IMAP]  
/hpop/imdircachesserv/ldapReplicationAgreement:  
[cn: RApop]  
[updateInterval: 60]  
[replArea: POP]  
/hwp/imdircachesserv/ldapReplicationAgreement:  
[cn: RAWp]  
[updateInterval: 60]  
[replArea: WP]
```

5. Set up your chaining configuration.

There is no chaining in this example.

5

Customizing the Directory Schema

The directory schema defines rules for the structure and values of the data that can be stored in the Directory database, and sets the rules that the Directory server and its clients use during search and update operations. In LDAP-based directories such as the InterMail Mx Integrated Services Directory (ISD), the schema is composed of object class and attribute definitions.

The standard InterMail ISD schema should meet most of your site-specific needs, and you should use the standard schema elements to structure as much of your data as possible. However, you can customize this schema by defining new object classes and attributes for your unique application.

Caution! Do not delete or change any standard schema object classes or attributes, and do not add new attributes to standard object classes. To group new attributes, define new object classes as described in “Creating Object Classes” on page 63. In order to modify the schema, you must have a good understanding of LDAP schema concepts, the standard ISD schema, and the types of queries and modifications you will be making to your data.

This chapter provides guidelines to help you customize the ISD schema. It covers:

- Customizing object classes
- Customizing attributes
- Schema checking
- Post-customization tasks

The LDAP schema is stored in the `cn=schema` entry in the Directory database. This entry contains the `subschema` object class. The two main attributes of this class are called `objectClasses` and `attributeTypes`. These are multi-valued attributes that define the object classes and attributes in the schema. For more information, see Chapter 7.

Note: For general information on schema design, see Chapter 7 of the textbook *Understanding and Deploying LDAP Directory Services* by T. Howes, M. Smith, and G. Good.

Customizing Object Classes

This section describes the types of LDAP object classes used in the standard ISD schema and details the procedure for defining new object classes to meet the unique needs of your organization.

About Object Classes

Object classes are used to group entries in a directory. They facilitate searches by providing a means for a directory client to retrieve a subset of directory entries that are instances of a particular object class. The ISD contains three types of object classes:

- Abstract
- Structural
- Auxiliary

An LDAP object class is defined by:

- A unique object identifier (OID)
- A name that uniquely identifies the class
- A class type
- Mandatory attributes
- Optional attributes

For example, the InterMail auxiliary object class `mailDomain` is defined as follows:

```
<OID for SWCOM>.2.2.2.4 NAME 'mailDomain' AUXILIARY
MUST (domainName $ domainType )
MAY (mailRelayHost $ mailRewriteDomain $ mailWildcardAccount) )
```

Where:

<OID for SWCOM>

Is 1.3.6.1.4.1.2415

Note: For information on obtaining an OID for your organization, see “Creating Object Classes” on page 63.

.2.2.2.4

Represents the portion of the OID for the `mailDomain` object class.

<code>mailDomain</code>	Is the class name. <i>Note: Names are case-insensitive.</i>
<code>AUXILIARY</code>	Is the class type.
<code>domainName</code> and <code>domainType</code>	Are mandatory attributes.
<code>mailRelayHost</code> , <code>mailRewriteDomain</code> , and <code>mailWildcardAccount</code>	Are optional attributes.

For more information on the format of object class definitions, see RFC 2252, which you can find at <http://www.rfc-editor.org/rfcsearch.html>.

Object classes are structured hierarchically, meaning that many of them are derived from other object classes. Understanding the object class hierarchy is crucial to defining new object classes correctly, since a child object class inherits all of the attributes of all of its superior (or ancestor) classes.

Figure 14 summarizes the hierarchy of the abstract and structural object classes in the InterMail ISD schema:

- `top` is superior to all the other object classes.
- `top` is the parent class of `person`.
- `person` is the parent class of `organizationalPerson`.
- `organizationalPerson` is the parent class of `inetOrgPerson`.

The dotted arrows show how the auxiliary object classes mix in with the structural object classes. For example, `adminTarget` and `mailDomain` can be mixed in with the `domain` structural object class.

For applications using LDAP, you can create additional combinations of object classes to define new directory objects. The ISD schema contains many object classes that you can use to create directory objects for your application. Chapter 7 describes these object classes.

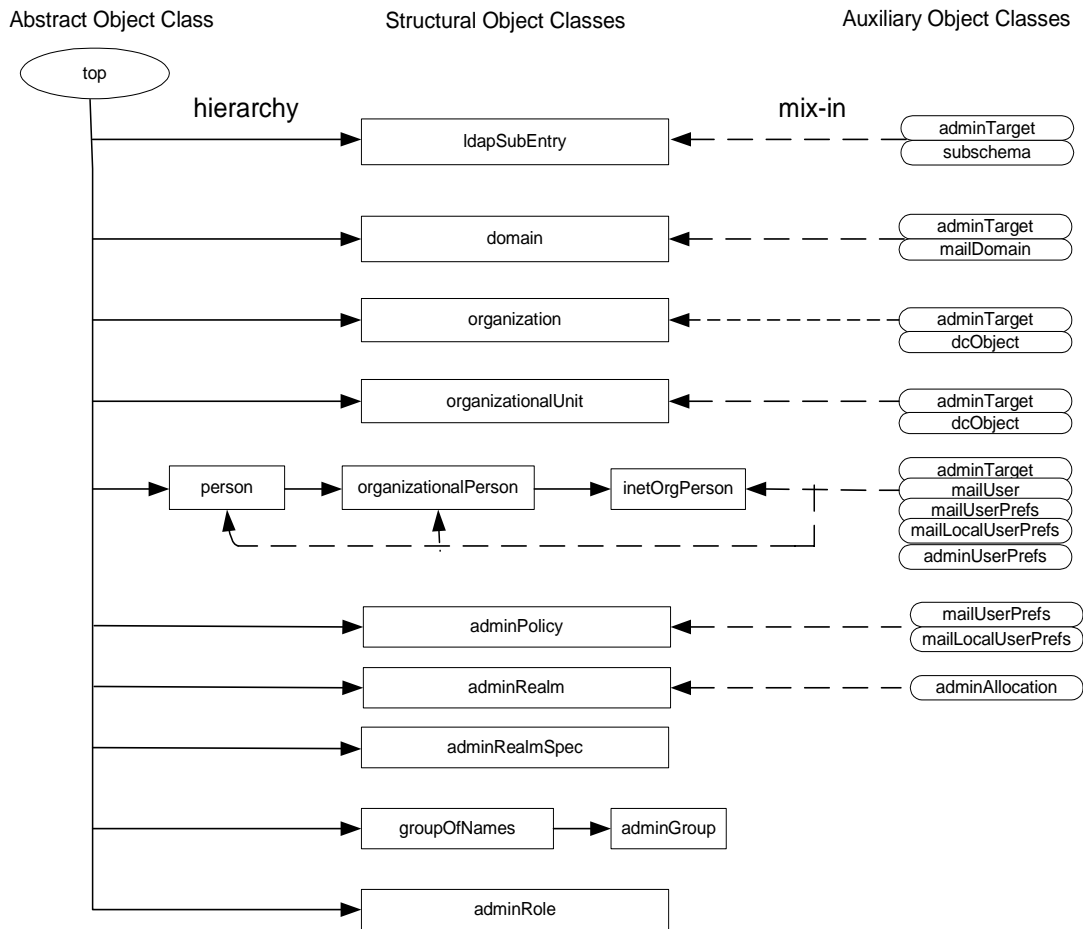


Figure 14 InterMail object classes

Abstract Object Classes

Abstract object classes are rare. They are superclasses used to group the other object classes, and they define attributes common to subordinate object classes. The `top` object class is an abstract class.

Structural Object Classes

Structural object classes define entries in the Directory Information Tree (DIT). All Directory database entries must include at least one structural class, but may also have auxiliary classes mixed in. The following InterMail object classes are structural classes:

- `adminGroup`
- `adminPolicy`

- adminRealm
- adminRole
- domain
- groupOfNames
- inetOrgPerson
- organization
- organizationalPerson
- organizationalUnit
- person
- ldapSubEntry

Auxiliary Object Classes

Auxiliary object classes, also called “mix-in” classes, add related attributes to a structural class entry. An auxiliary object class can be mixed in with any structural object class. The following InterMail object classes are auxiliary classes:

- adminAllocation
- adminTarget
- adminUserPrefs
- dcObject
- mailDomain
- mailLocalUserPrefs
- mailUser
- mailUserPrefs
- subschema

Creating Object Classes

You create new object classes with the standard LDAP utility `ldapmodify`, described in Chapter 9. When you create a new object class, you are modifying the schema object entry (`cn=schema`) by adding a value to the `objectClasses` attribute.

Each new object class definition must follow these rules:

- The name must be unique.
- The object identifier (OID) should be a number assigned to your organization by the Internet Assigned Numbers Authority (IANA). You can find a form for requesting an OID at <http://www.isi.edu/cgi-bin/iana/enterprise.pl>.
- The new object class cannot be superior to any existing object class. If it were, it would change the characteristics of everything below it in the hierarchy.
- An alias can be added to an attribute definition using the `attributeAliasingEnable` configuration key described in Chapter 8.

To define a new structural object class called `newclass`:

1. Create an LDIF file to define the new object class. For example:

```
dn: cn=schema
changeType: modify
add: objectClasses
objectClasses: ( <OID#> NAME <newclass> SUP <parentclass>
STRUCTURAL
MUST (<mandatory_attribute1> $ <mandatory_attribute2> $
<mandatory_attribute3>)
MAY (<optional_attribute1> $ <optional_attribute2>))
```

Where:

<code>cn=schema</code>	Is the distinguished name of the LDAP object being modified, in this case the schema.
<code>changeType: modify</code>	Tells the Directory server to modify the schema object.
<code>add: objectClasses</code>	Tells the Directory server to add a new attribute value to the <code>objectClasses</code> attribute. <i>Note: Adding a new object class always involves modifying (adding a value to) the <code>objectClasses</code> attribute of the schema object.</i>
<code>objectClasses:</code>	Defines the name of the schema attribute being modified as <code>objectClasses</code> .
<code><OID#></code>	Is the OID of the new object class. Use a number assigned to your organization by the Internet Assigned Numbers Authority (IANA).
<code>NAME <newclass></code>	Defines the name of the new object class as <code><newclass></code> .
<code>SUP <parentclass></code>	Defines the superior (or parent) object class of <code><newclass></code> as <code><parentclass></code> . You can determine the parent object class by looking at Figure 14.
<code>STRUCTURAL</code>	Defines <code><newclass></code> as a structural object class.
<code>MUST (<mandatory_attribute1> \$ <mandatory_attribute2> \$ <mandatory_attribute3>)</code>	Lists the attributes that must be defined for this object class, separated by \$. This list must be enclosed in ().

MAY (<optional_attribute1> \$ <optional_attribute2>)) Lists the optional attributes for this object class, separated by \$. This list must be enclosed in ().

Note: The technical specification for LDIF can be found at <http://search.ietf.org/internet-drafts/draft-good-ldap-ldif-05.txt>.

2. Give the LDIF file a name.
3. Use the `ldapmodify` command to modify the `objectClasses` attribute:

```
-D <managerBindDN> -w <password>
ldapmodify -f <class_filename.ldif>
```

Where:

`-D <managerBindDN> -w <password>` Are the login parameters, that is, the distinguished name used for binding to the directory and the password.

`-f <class_filename>` Tells the Directory server to read the entry modification from the file `<class_filename.ldif>`.

Customizing Attributes

This section describes the characteristics of the LDAP attributes used in the standard ISD schema and details the procedures for defining new attributes.

About Attributes

An attribute is information describing one trait of a directory entry. It can belong to one or more object classes. Each attribute in an object has a name and one or more values. For example, in a `person` directory object, the `telephonenumber` attribute can have values such as `<123-456-7890>` and `<321-7654>`.

In the schema, each attribute is described in terms of the following characteristics:

- Whether the attribute has a single value only or can have multiple values
- The syntax to which the values must conform
- Matching rules for attribute values in searches

The attribute value is the actual data associated with the attribute in a Directory database entry. The attribute must follow the syntax rule specified in the attribute definition. For example, for an attribute having the syntax `integer`, the values must be digits. The LDAP protocol places no restrictions on the format, length, or type of data associated with attributes. However, some attributes have constraints placed on them to limit their size or the number of values they may have.

Attributes in the ISD can follow any of the syntax rules listed in RFC 2252, section 4.3.2, which you can find at <http://www.rfc-editor.org/rfcsearch.html>. The ISD schema represents each of these syntax rules with a numeric string.

The syntax rules encountered most often in the ISD, and their numeric strings, are:

Syntax Rules	Associated Numeric String
Boolean	1.3.6.1.4.1.1466.115.121.1.7
Directory string	1.3.6.1.4.1.1466.115.121.1.15
Distinguished name	1.3.6.1.4.1.1466.115.121.1.12
Generalized time	1.3.6.1.4.1.1466.115.121.1.24
IA5 string	1.3.6.1.4.1.1466.115.121.1.26
Integer	1.3.6.1.4.1.1466.115.121.1.27
Numeric string	1.3.6.1.4.1.1466.115.121.1.36
Octet string	1.3.6.1.4.1.1466.115.121.1.40
Printable string	1.3.6.1.4.1.1466.115.121.1.44

In LDAP searches, a server compares an attribute value with the value in its search filter according to the matching rule defined for the attribute. For example, if an attribute has the matching rule `caseIgnoreMatch`, the Directory server ignores the case when it compares the value in the search filter with the value stored in the database. The matching rule thus plays a role in whether the search or authentication is successful.

Matching rules used for the attributes in the ISD include:

- `booleanMatch`
- `caseExactMatch`
- `caseIgnoreIA5Match`
- `caseIgnoreMatch`
- `distinguishedNameMatch`
- `integerMatch`
- `numericStringMatch`
- `objectIdentifierMatch`
- `octetStringMatch`

For example, the ISD schema defines the attribute `domainName` like this:

```
attributetypes: (1.3.6.1.4.1.2415.2.2.1.4
NAME 'domainName'
EQUALITY caseIgnoreMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 {255} SINGLE-VALUE)
```

Where:

<code>attributetypes:</code>	Signifies that you are defining an attribute.
<code>1.3.6.1.4.1.2415.2.2.1.4</code>	Is the OID number for this attribute
<code>NAME 'domainName'</code>	Defines the name of the attribute as <code>domainName</code> .
<code>EQUALITY caseIgnoreMatch</code>	Defines the matching rule (EQUALITY) this attribute must follow as <code>caseIgnoreMatch</code> .
<code>SYNTAX</code> <code>1.3.6.1.4.1.1466.115.121.1.26</code>	Defines the syntax of this attribute as <code>IA5string</code> , as shown in the table on page 66 and in RFC 2252.
<code>{255}</code>	Constrains the maximum number of characters this string can have to 255.
<code>SINGLE-VALUE</code>	Means that this attribute can have only one value.

For more information regarding the `domainName` attribute, see the description of the `mailDomain` object class in Chapter 7. For an alphabetical list of all the attributes in the InterMail Directory database, also see Chapter 7.

Adding New Attributes

You can add a new attribute to the ISD schema by doing any of the following:

- Defining a new attribute in the schema.
- Adding a new attribute to an existing object class you previously defined.
- Adding a new class-of-service attribute to the `mailLocalUserPrefs` object class. Initially empty, this object class is used to group new attributes that define user preferences. These new attributes are treated just like the attributes in the `mailUserPrefs` object class described in Chapter 7.

Caution! Do not add new attributes to existing standard object classes. You may add attributes only to `mailLocalUserPrefs` and to object classes that you have defined yourself.

Defining a New Attribute in the Schema

To define a new attribute in the schema:

1. Create an LDIF file to define the new attribute. For example:

```
dn: cn=schema
changeType: modify
add: attributeTypes
attributeTypes: ( <OID#> NAME <newattribute> EQUALITY
<matchingrule> SYNTAX 1.3.6.1.4.1.1466.115.121.1.<#>
[SINGLE-VALUE|MULTI-VALUE] )
```

Where:

dn: cn=schema	Represents the distinguished name of the LDAP object being modified as cn=schema.
changeType: modify	Tells the Directory server to modify the schema object.
add: attributeTypes	Tells the Directory server to add a new attribute called attributeTypes to the schema object. <i>Note: Adding a new attribute always involves modifying the attribute attributeTypes of the object class schema. For more information on this attribute, see Chapter 7.</i>
attributeTypes:	Defines the name of the schema attribute being modified as attributeTypes.
<OID#>	Is the OID of the new attribute. Use a number assigned to your organization by the Internet Assigned Numbers Authority (IANA).
NAME <newattribute>	Defines the name of the new attribute as <newattribute>. <i>Note: You listed <newattribute> as a mandatory or optional attribute of the object class <newclass> when you defined this new object class.</i>
EQUALITY <matchingrule>	Defines the matching rule for <newattribute>, for example, caseIgnoreMatch.

<p>SYNTAX 1.3.6.1.4.1.1466.115.121.1.<#></p>	<p>Defines the syntax for <newattribute>.</p> <p>Note: Replace # with the appropriate number as defined in RFC 2252 and on page 66.</p>
<p>[SINGLE-VALUE MULTI-VALUE]</p>	<p>Defines <newattribute> as a single- or multi-valued attribute.</p> <p>Note: If you do not include this parameter, a multi-valued attribute is assumed.</p>

2. Give the LDIF file a name.
3. Use the `ldapmodify` command to modify the `attributeTypes` attribute in the schema:

```
-D <managerBindDN> -w <password>
ldapmodify -f <attrib_filename.ldif>
```

Where:

<pre>-D <managerBindDN> -w <password></pre>	<p>Are the login parameters, that is, the distinguished name used for binding to the directory and the password.</p>
<pre>-f <attrib_filename.ldif></pre>	<p>Tells the Directory server to read the entry modification from the file <attrib_filename.ldif>.</p>

Adding a New Attribute to an Object Class You Created Previously

To add a new attribute to an object class that you have previously defined:

1. Create an LDIF file to add the new attribute.
 - a. Delete the previously-defined object class.

Note: Make sure you have an up-to-date backup copy of the schema before you delete any parts of it.

- b. Redefine the object class with the new attribute.

Note: You can add optional attributes to an object class you created previously, but you cannot add mandatory attributes.

You perform these two steps with a single modify request. For example:

```
dn: cn=schema
changeType: modify
delete: objectClasses
objectClasses: (<OID#> NAME '<customOC>' SUP <parentOC>
[STRUCTURAL | AUXILIARY | ABSTRACT]
MUST (<mandatory_attr1> $ <mandatory_attr2>)
MAY (<optional_attr1>))
-
add: objectClasses
objectClasses: (<OID#> NAME '<customOC>' SUP <parentOC>
[STRUCTURAL | AUXILIARY | ABSTRACT]
MUST (<mandatory_attr1> $ <mandatory_attr2>)
MAY (<optional_attr1> $ <optional_attr2>))
```

Where:

dn: cn=schema	Is the distinguished name of the LDAP object being modified, in this case the schema.
changeType: modify	Tells the Directory server to modify the schema object.
delete: objectClasses	Tells the Directory server to delete objectClasses from the schema.
objectClasses:	Signifies that the name of the schema attribute being deleted is objectClasses. <i>Note: Deleting an object class entails modifying the attribute called objectClasses of the object class schema. For more information, see Chapter 7.</i>
<OID#>	Is the OID of the object class being modified. Use a number assigned to your organization by IANA.
NAME '<customOC>'	Defines the name of the object class being modified as <customOC> (enclosed in ' ').
SUP <parentOC>	Signifies that the name of the superior (or parent) object class of <customOC> is <parentOC>.
[STRUCTURAL AUXILIARY ABSTRACT]	Specifies whether the object class being modified is structural, auxiliary, or abstract.

MUST (<mandatory_attr1> \$ <mandatory_attr2>)	Lists all of the attributes that must be defined for this object class, separated by \$. This list must be enclosed in ().
MAY (<optional_attr1>)	Lists the existing optional attribute for this object class, which must be enclosed in ().
-	Separates the delete and add operations.
add: objectClasses	Tells the Directory server to add the objectClasses attribute to the schema.
objectClasses:	Signifies that objectClasses is the name of the schema attribute being added.
(<optional_attr1> \$ <optional_attr2>)	Lists the optional attributes for this object class, separated by \$. This list must be enclosed in (). <optional_attr2> is the new attribute you are adding. <i>Note: You must respecify the existing attributes in addition to the new attributes.</i>

2. Give the LDIF file a name.
3. Use the ldapmodify command to modify the attributeTypes attribute:

```
-D <managerBindDN> -w <password>
ldapmodify -a -f <attrib_filename.ldif>
```

Adding a New Class-of-Service Attribute

To add a new class-of-service attribute to the mailLocalUserPrefs object class:

1. Create an LDIF file to add the new COS attribute:
 - a. Delete the mailLocalUserPrefs object class.
 - b. Redefine the mailLocalUserPrefs object class with the new attribute.

You perform these two steps with a single modify request. For example:

```
dn: cn=schema
changeType: modify
delete: objectClasses
objectClasses: ( 1.3.6.1.4.1.2415.2.2.2.12
NAME 'mailLocalUserPrefs'
SUP top AUXILIARY)
-
add: objectClasses
objectClasses: ( 1.3.6.1.4.1.2415.2.2.2.12 NAME
'mailLocalUserPrefs' SUP top AUXILIARY MAY <mailNewPref>
```

Where:

dn: cn=schema	States that the distinguished name of the LDAP object being modified is cn=schema, meaning that you are modifying the schema.
changeType: modify	Tells the Directory server to modify the schema object.
delete: objectClasses	Tells the Directory server to delete objectClasses from the schema.
objectClasses:	Signifies that the name of the schema attribute being deleted is objectClasses. <i>Note: Deleting an object class entails modifying the attribute called objectClasses of the object class schema. For more information, see Chapter 7.</i>
1.3.6.1.4.1.2415.2.2.2.12	Is the OID of the mailLocalUserPrefs object class.
NAME 'mailLocalUserPrefs'	Signifies that the name of the object class being modified is mailLocalUserPrefs.
SUP top	Specifies that the superior (or parent) object class of mailLocalUserPrefs is top.
AUXILIARY	Specifies that mailLocalUserPrefs is an auxiliary object class.
-	Separates the deletion step from the addition step.
add: objectClasses	Tells the Directory server to add objectClasses to the schema.
objectClasses:	Signifies that objectClasses is the name of the schema attribute being added.
MAY <mailNewPref>	Tells the Directory server that mailLocalUserPrefs has one optional attribute called <mailNewPref>. <i>Note: You must respecify any existing attributes that you may have defined previously in addition to adding the new attributes.</i>

2. Give the LDIF file a name, such as <attrib_filename.ldif>.
3. Use the `ldapmodify` command to modify the `attributeTypes` attribute:

```
-D <managerBindDN> -w <password>
ldapmodify -a -f <attrib_filename.ldif>
```

Defining Attribute Constraints

You may wish to add constraints to some of the attributes you define. Attribute constraints are used to:

- Limit the number of characters in a string
- Limit the number of attribute values to a single value
- Limit attribute values to a range of values
- Limit attribute values to specific choices

To limit the number of characters in the value of an attribute, insert a number enclosed in braces after the syntax numeric string in the attribute definition. For example:

```
attributeTypes: ( <attribute_OID> NAME <attribute_name>
EQUALITY <matching_rule> SYNTAX <1.2.3.4.5.6.7{256}>
SINGLE_VALUE )
```

Where:

{256} Is the maximum number of characters in the value of this attribute.

To limit the number of attribute values to one, insert the term `SINGLE-VALUE` after the syntax definition, as shown in the previous example.

To limit attribute values to a range of numbers, insert the term `X-VALUE-CONSTRAINT` followed by `'RANGE, <range of values>'` into the attribute definition. For example:

```
attributeTypes: ( <attribute_OID> NAME <attribute_name> EQUALITY
<matching_rule> SYNTAX <1.2.3.4.5.6.7> SINGLE_VALUE
X-VALUE-CONSTRAINT 'RANGE,0-1')
```

To limit attribute values to specific choices, insert the term `X-VALUE-CONSTRAINT` followed by `'CHOICE, <choiceA, choiceB, choiceC>'`. For example:

```
attributeTypes: ( <attribute_OID> NAME <attribute_name> EQUALITY
<matching_rule> SYNTAX <1.2.3.4.5.6.7> SINGLE_VALUE
X-VALUE-CONSTRAINT 'CHOICE, A,D,S,L,M,P')
```

This attribute can have any one of the values A, D, S, L, M, or P.

Schema Checking

Schema checking is the process of checking a newly created or modified LDAP entry before writing it to the Directory database to ensure that all data added to the Directory database complies with the rules defined in the schema.

When the Directory server is initialized, the `imdirmake` utility:

1. Reads the ISD schema from the `schema.ldif` file.
2. Writes the schema in the `cn=schema` entry in the Directory database.

When the Directory server comes up, it:

1. Reads the schema from the Directory database.
2. Uses the schema to check new and modified data before it is added to the Directory database.

The Directory server checks all new and modified Directory database entries against the schema to ensure that:

- Each entry contains the mandatory attributes of all specified object classes and their superior object classes.
- Each entry contains only the mandatory and optional attributes specified in the object class definitions. No other attributes are allowed.
- Each attribute has the syntax and number of values (single or multiple) specified in the schema definition file.
- Attributes conform to their constraints.

The schema checking process is turned on by default for the Directory server. The `ldapSchemaCheck` configuration key should always remain set to `true`.

Schema changes made in the Directory server are automatically replicated to all Directory Cache servers.

Note: Schema checking enforces the rules for schema entries. When you provision data, it ensures that attributes and their values comply with schema definitions, but it does not tell you whether your definitions make sense. For example, if you create a new object class, schema checking cannot tell you whether it is placed properly in the object class hierarchy. If you create a new attribute, schema checking cannot tell you whether it is defined correctly for your purpose.

Post-Customization Tasks

After you add new attributes to the schema, they are referenced and utilized by the Directory server and the Directory Cache servers in various ways:

- Replication agreements specify which Directory database entries are copied and maintained by a particular Directory Cache server. For more information on replication agreements, see Chapter 4.
- Attribute indexing improves the efficiency of directory searches by limiting them to indexed attributes. For more information on attribute indexing, see Chapter 3.
- Access Control Information (ACI) rules protect directory entries from unauthorized tampering. You specify ACI rules for a specific object class or attribute in order to allow or deny read or write access by a user or group of users. For more information on ACI rules, see Chapter 2.
- Allocation rules define the attributes used to count and limit services, such as the number of accounts or the number of users with certain types of access. For more information on allocation rules, see Chapter 6.

You must be sure to consider these factors when you customize the ISD schema.

6

Customizing the DIT

A Directory Information Tree (DIT) is the hierarchical structure dictated by the LDAP standard to organize directory entries. It takes the form of an inverted tree, with the root at the top and the branches and leaves below it. InterMail includes an initial DIT, which is created with the script in the `init_dit.ldif` file when InterMail is installed. You can customize InterMail's initial DIT to meet the needs of your organization.

This chapter provides guidelines to help you customize the InterMail DIT. It covers:

- About InterMail's Initial DIT
- Customizing DIT Entries

About InterMail's Initial DIT

The InterMail DIT represents the structure of the Directory database. Each entry in the DIT has a distinguished name (DN) that uniquely identifies it within the tree, and a relative distinguished name (RDN) that uniquely identifies it among its peers at the same node in the tree. An entry's DN consists of a chain of the RDNs of each node in its path, in the form of <attribute name> = <attribute value> pairs separated by commas. The leaf entry is on the left, with the remaining RDNs going up through the tree to the root on the right.

Note: This structure is the opposite of that of files in an operating system, where the path goes from the highest-level directory on the left down to the specific name on the right.

Figure 15 shows InterMail's initial DIT.

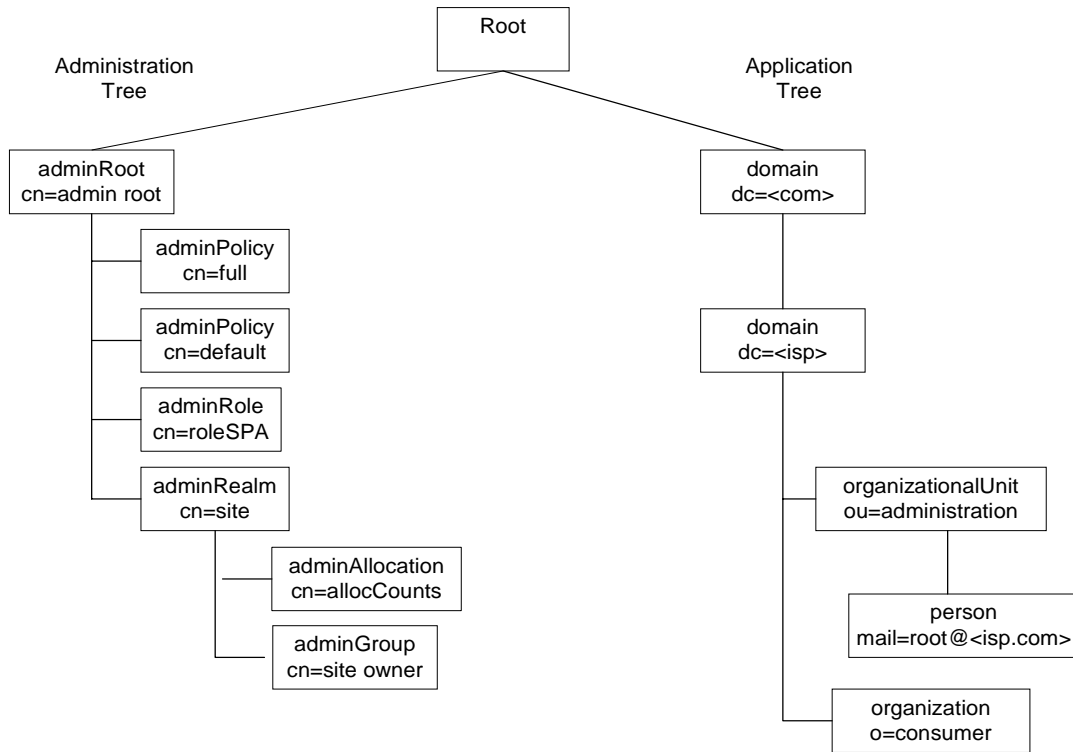


Figure 15 InterMail's Initial DIT

InterMail's initial DIT is separated into two parts, the administration tree and the application tree. The administration tree, which is the branch on the left side, contains account management information such as class of service, administrative group, and access control privileges required for InterMail administration. The administration tree component of the initial DIT defines the minimum set of entries necessary to run InterMail.

The application tree, which is the branch on the right side, contains the information that is returned to users as a result of Directory database queries, such as person entries, organizations, and domains.

The initial DIT consists of only the skeletal information structure. You customize the DIT by adding leaf nodes to the bottom of the tree structure.

About the Administration Tree

The following table lists the object classes and distinguished names in the initial DIT's administration tree, and a description of what each represents.

Object Class	Distinguished Name	Description
adminRoot	cn=admin root	This entry is the structural root of the administration tree. It also contains the allocation rules, which determine the attributes to be counted and the maximum values of those attributes.
adminPolicy	cn=full	This entry defines the initial class of service that has the maximum (full) set of permissions. A class of service is a set of access permissions, quotas, and default preferences for a group of users. You can modify the full class of service or create new classes of service from it. You can associate new accounts with this adminPolicy or any other newly created adminPolicy.
adminPolicy	cn=default	This entry defines the default class of service, which is used only if an account has no adminPolicy assigned. You should not modify the default adminPolicy entry.
adminRole	cn=roleSPA	This entry defines the role associated with the Supervisory Provider Administrator. <i>Note: The initial DIT also defines other administrative roles. Their common names (cn) are: rolePA, roleSCSR, roleCSR, roleSOA, roleOA, roleOUA, roleGA, and roleHOH. See "Defining Administrative Roles" on page 97 for more information on these roles.</i>
adminRealm	cn=site	This entry defines the realm associated with the site provider licensing InterMail. All other realms are subordinate to this one in the DIT.
adminAllocation	cn=allocCounts	This entry defines the maximum values for attributes whose values you wish to count, as well as data on current usage. <i>Note: The initial allocation entries are specified in the init_allocations.ldif file, not the init-dit.ldif file.</i>
adminGroup	cn=site owner	This entry defines the administrative group for role SPA to which administrators can be added.

About the Application Tree

The following table lists the object classes and distinguished names in the initial DIT's application tree, and a description of what each represents:

Object Class	DN	Description
domain	dc=<com>	This entry defines the last part of the domain name for commercial e-mail accounts. For example, for Software.com, you would use dc=com.
domain	dc=<isp>	This entry defines the first part of the domain name for e-mail accounts. This represents the organization that has licensed InterMail. For example, if an organization called ISP.com licenses InterMail, this entry would be dc=ISP.
organizationalUnit	ou=administration	This entry contains the person entries for the first administrator created when the directory is installed.
person	mail=root@<isp.com>	This entry contains the person entries that correspond to the super user administrator.
organization	o=consumer	This entry contains the person entries for the consumer (non-business) mail customers of the ISP.

The entries in the InterMail application tree are constructed from the object classes described in Chapter 5.

Customizing DIT Entries

You can customize the DIT to meet your organization's unique needs by modifying the DIT in the following ways. The order of this list corresponds to the sequence of actions most commonly used by administrators.

- Adding domains, organizations, and organizational units to the application tree
- Modifying the Access Control Information (ACI) rules
- Adding administrative groups
- Adding administrators to an administrative group
- Adding administrative policies (classes of service)
- Adding attribute constraints to an existing administrative policy
- Modifying attribute constraints

- Modifying or adding class-of-service attributes
- Modifying the allocation rules specifying which attributes are counted
- Defining administrative roles

Caution! You may add leaf entries only. You may modify only those entries that you make yourself. Do not delete any entries in the initial DIT.

Adding Domains

You add new domains to your DIT in order to set up mail accounts for a new customer or to provide an additional network address for an existing customer.

To add a new domain:

1. Create an LDIF file to add the new domain:

```
dn: dc=<isp>, dc=<com>
dc: <isp>
objectClass: top
objectClass: domain
objectClass: mailDomain
objectClass: organization
domainName: <CompanyA>.<com>
domainType: <L>
o: <CompanyA>
```

Where:

`dn:dc=<isp>, dc=<com>`

Is the distinguished name of the new domain.

`dc: <isp>`

Is the domain component representing the name of the ISP or other company.

`objectClass: top`
`objectClass: domain`
`objectClass: mailDomain`
`objectClass: organization`

Are the object classes containing the attributes you are adding.

`domain` is the structural object class that identifies the owner of a network address. It contains the `dc` attribute.

`top` is the parent class of `domain`.

`mailDomain` is an auxiliary class that is mixed-in with `domain` to create a DNS domain name for an InterMail e-mail address. It contains the `domainName` and `domainType` attributes.

`organization` is the structural object class that identifies the company or other top level institution. (It contains the `o` attribute.)

domainName: <CompanyA>.<com>	Is the complete domain name you are adding.
domainType: <L>	Defines the new domain as a Local domain.
o: <CompanyA>	Identifies the organization that owns the new domain. <i>Note: This is an optional attribute.</i>

Note: The technical specification for LDIF can be found at <http://search.ietf.org/internet-drafts/draft-good-ldap-ldif-05.txt>.

2. Save this LDIF file.
3. Use the `ldapadd` command to add the new domain:

```
ldapadd -D <binddn> -w <password> -f <filename>
```

Where:

-D <binddn>	Uses <binddn> to bind to the directory. <binddn> should be a DN as defined in RFC 1779.
-w <password>	Uses <password> as the password for simple authentication
-f <filename>	Specifies the name of the LDIF file you just created as the source of a new entry in the Directory database.

Adding Organizations

You add a new organization when you add accounts to the Directory database for a new customer. You can enter the new organization as a domain component (see “Adding Domains” on page 81), or you can enter it as an organization entry, as follows:

To add a new organization entry:

1. Create an LDIF file to add the new organization:

```
dn: o=<isp>, dc=<isp>, dc=com  
o: <isp>  
objectClass: top  
objectClass: organization
```

Where:

dn:o=<isp>, dc=<isp>,dc=com	Is the distinguished name of the new organization.
o: <isp>	Is the name of the new organization.

objectClass: top	Is the parent object class of organization
objectClass: organization	Is the object class that corresponds to a company or other top level institution.

2. Save this LDIF file.
3. Use the `ldapadd` command to add the new organization:

```
ldapadd -D <binddn> -w <password> -f <filename>
```

Where:

-D <binddn>	Uses <binddn> to bind to the directory. <binddn> should be a DN as defined in RFC 1779.
-w <password>	Uses <password> as the password for simple authentication
-f <filename>	Specifies the name of the LDIF file you just created as the source of a new entry in the Directory database.

Adding Organizational Units

You add a new organizational unit when you want to group person entries by department, regional office, or any other characteristic.

To add a new organizational unit:

1. Create an LDIF file to add the new organizational unit:

```
dn:ou=<new_ou>,dc=<isp>,dc=<com>
ou: <new_ou>
objectClass: top
objectClass: organizationalUnit
```

Where:

dn:ou=<new_ou>, dc=<isp>, cd=<com>	Is the distinguished name of the new organizational unit. <i>Note: In this example, we add the new organizational unit underneath a domain component. You can also add organizational units underneath an organization or under other organizational units.</i>
ou: <new_ou>	Is the name of the new organizational unit.
objectClass: top	Is the parent object class of organizationalUnit.

`objectClass: organizationalUnit` Is the object class that corresponds to a department, regional office, or other subdivision of an organization.

2. Save this LDIF file.
3. Use the `ldapadd` command to add the new organizational unit:

```
ldapadd -D <binddn> -w <password> -f <filename>
```

Where:

`-D <binddn>` Uses `<binddn>` to bind to the directory. `<binddn>` should be a DN as defined in RFC 1779.

`-w <password>` Uses `<password>` as the password for simple authentication

`-f <filename>` Specifies the name of the LDIF file you just created as the source of a new entry in the Directory database.

Modifying Access Control Information Rules

The initial DIT defines Access Control Information (ACI) rules that specify who can and cannot read or modify a particular DIT entry. These rules take the following form:

```
aciRule: <bindDN>, <bindType>, <objectClass>, <attribute>, <scope>, <permissions>
```

Where:

`bindDN` Is a distinguished name that uniquely identifies the user in the Directory. A null value ("") indicates the `root` user.

`bindType` Can be yourself, a group, or a subtree of the DIT.

Values:

`self`
`group`
`subtree`

`objectClass` Is the object class in the Directory schema that you want to access. A null value (" ") indicates all object classes.

Note: See Chapter 7 for a list and description of InterMail object classes.

`attribute` Is the attribute in the Directory schema that you want to access. A null value ("") indicates all attributes.

Note: See Chapter 7 for a list and description of InterMail attributes.

scope	Specifies whether the rule applies only to the entry specified, or to all of its child entries also. Values: entry children
permissions	Are the access rights to be allowed or denied Values: ar to allow read access aw to allow write access aar to allow read access and the right to delegate read access to another user aaw to allow write access and the right to delegate write access to another user

The root entry of the initial DIT contains the following ACI rules:

ACI Rule 1

```
aciRule:<"cn=site owner,cn=site,cn=admin root",group,"",
",children,aar+aaw>
```

This rule gives the members of the site owner administrative group permission to delegate read and write access to all object classes and attributes for all Directory database entries.

ACI Rule 2

```
aciRule:<"",self,"","",children,ar>
```

This rule gives all users read access to all object classes and attributes in the entries for their own accounts.

The other ACI rules are part of the entry to be modified. For example:

```
dn: cn=full, cn=admin root
cn=full
objectclass: top
objectclass: adminPolicy
objectclass: mailUserPrefs
aciRule:<"",subtree,"","",entry,ar>
```

This rule gives all users whose accounts have the highest class of service (called full) read access to all object classes and attributes in this adminPolicy.

You can add, delete, or modify ACI rules with the `ldapmodify` utility. When you define a new ACI rule, you are modifying the value of the `aciRule` attribute in an entry.

You add a new ACI rule when you want to allow or disallow a particular user or group of users to read or modify a particular DIT entry.

To add a new ACI rule:

1. Create an LDIF file to add the new ACI rule:

```
dn: <entry to be modified>
changeType: modify
add: aciRule
aciRule: <bindDN>, <bindType>, <objectClass>,<attribute>, <scope>,
<permissions>
```

Where:

<code>dn:<entry to be modified></code>	Is the distinguished name (DN) of the entry you want to modify (called the <code>targetDN</code>).
<code>changeType:modify</code>	Indicates that you are modifying an entry.
<code>add: aciRule</code>	Indicates that you are adding an <code>aciRule</code> attribute to the DIT.
<code>aciRule: <bindDN>,<bindType>, <objectClass>,<attribute>, <scope>,<permissions></code>	Is the new ACI rule.

2. Save this LDIF file.
3. Use the `ldapmodify` command to add the new ACI rule:

```
ldapmodify -D <binddn> -w <password> -f <filename>
```

Where:

<code>-D <binddn></code>	Uses <code><binddn></code> to bind to the directory. <code><binddn></code> should be a DN as defined in RFC 1779.
<code>-w <password></code>	Uses <code><password></code> as the password for simple authentication.
<code>-f <filename></code>	Specifies the name of the LDIF file you just created as the source of a new entry in the Directory database.

Adding Administrative Groups

You add a new administrative group to create a new set of administrators whose role and privileges are different than those of existing administrative groups within the same realm.

It is recommended that you add a new administrative group through the InterManager GUI. However, you can also add a new administrative group using the standard LDAP utility `ldapadd` described in Chapter 9.

To add a new administrative group:

1. Create an LDIF file to define the new administrative group:

```
dn: cn=<newGroup>, cn=site, cn=admin root
cn: <newGroup>
objectClass: top
objectClass: groupOfNames
objectClass: adminGroup
adminRoleDN: <adminRoleDN>
adminAllowedAdminPolicyDN: <adminPolicyDN>
member: <memberDN>
```

Where:

dn: cn=<newGroup>, cn=site, cn=admin root	Is the distinguished name of the new administrative group.
cn: <newGroup>	Is the common name of the new administrative group.
objectClass: top objectClass: groupOfNames	Are the ancestor object classes of the adminGroup object class. This means that the adminGroup object class is derived from groupOfNames and top, and inherits the characteristics of these two object classes.
objectClass: adminGroup	Is the object class for administrative groups.
adminRoleDN: <adminRoleDN>	Is a mandatory attribute of the adminGroup object class. It describes the generic privileges of this administrative group by specifying the distinguished name of a corresponding adminRole for this group. Example: adminRoleDN: <cn=rolePA, cn=admin root>
adminAllowedAdminPolicyDN: <adminPolicyDN>	Is the distinguished name that determines the class of service for an account in the group. You can specify multiple adminAllowedAdminPolicyDNs to represent different classes of service for various accounts in the administrative group. Example: adminAllowedAdminPolicyDN: <cn=full, cn=admin root> represents the highest level class of service, having a full range of permissions.

member: <memberDN> Identifies the person entries (members) of this administrative group.

Example:

```
member: <mail=root@isp.com,  
ou=administration, dc=isp, dc=com>
```

2. Save this LDIF file.
3. Use the `ldapadd` command to add the new administrative group:

```
ldapadd -D <binddn> -w <password> -f <filename>
```

Where:

-D <binddn> Uses <binddn> to bind to the directory. <binddn> should be a DN as defined in RFC 1779.

-w <password> Uses <password> as the password for simple authentication

-f <filename> Specifies the name of the LDIF file you just created as the source of a new entry in the Directory database.

Adding Administrators

You add a member to an administrative group when you add personnel having the same role as the other members of the group, or when you create a new group. For example, for a new department, you might add a new customer service representative or a new organizational unit administrator.

To add an administrator to an administrative group, use the standard LDAP utility `ldapmodify`, described in Chapter 9.

Note: This example assumes that the person entry for the new administrator already exists, and gives him new administrative permission.

To add a new administrator:

1. Create an LDIF file to add the new administrator:

```
dn: cn=<groupName>, cn=site, cn=admin root  
changeType: modify  
add: member  
member: <newPerson>
```

Where:

dn: cn=<groupName>, cn=site, cn=admin root Is the distinguished name of the administrative group <groupName>.

changeType: modify Indicates that you are modifying an entry.

add: member	Indicates that you are adding a person to the administrative group.
member: <newPerson>	Is the distinguished name of the new member of the administrative group.

2. Save this LDIF file.
3. Use the `ldapmodify` command to add the new administrator:

```
ldapmodify -D <binddn> -w <password> -f <filename>
```

Where:

-D <binddn>	Uses <binddn> to bind to the directory. <binddn> should be a DN as defined in RFC 1779.
-w <password>	Uses <password> as the password for simple authentication.
-f <filename>	Specifies the name of the LDIF file you just created as the source of a new entry in the Directory database.

Adding Administrative Policies

Administrative policies represent classes of service in the DIT. You add a new `adminPolicy` entry to create a new class of service if you want to define a new combination of access permissions and services for a group of users.

Note: The following list of `adminPolicy` attributes represents the default class of service, which has full administrative permission.

To add a new administrative policy:

1. Create an LDIF file to define the new `adminPolicy`:

```
dn: cn=<newPolicy>, cn=admin root
cn: <new Policy>
objectClass: top
objectClass: adminPolicy
objectClass: mailUserPrefs
mailAutoReplyMode: <N>
mailDeliveryOption: <P>
mailForwarding: <0>
mailImapAccess: <all>
mailImapSslAccess: <all>
mailInterManager: <1>
mailInterManagerSsl: <1>
mailLdapAccess: <all>
mailMtaFilter: <0>
mailMtaFilterPerUser: <0>
mailParentalControl: <1>
mailPopAccess: <all>
```

```
mailPopSslAccess: <all>
mailQuotaBounceNotify: <1>
mailQuotaMaxMsgKB: <100>
mailQuotaMaxMsgs: <1000>
mailQuotaThreshold: <70>
mailQuotaTotKb: <10000>
mailSelfCare: <1>
mailSelfCareSsl: <1>
mailSmtAccess: <1>
mailSmtAuth: <0>
mailSmtSslAccess: <1>
mailWebmailAccess: <1>
mailWebmailUseSignature:<1>
<list of adminAttributeConstraints>
description: <text description of this administrative
policy>
```

Where:

dn: cn=<newPolicy>, cn=admin root	Is the distinguished name of the new administrative policy.
cn: <new Policy>	Is the common name of the new administrative policy.
objectClass: top	Is the parent object class of adminPolicy.
objectClass: adminPolicy	Is the object class that contains the administrative policy.
objectClass: mailUserPrefs	Is the object class that contains mail user preferences for a class of service.

```
mailAutoReplyMode: <N>
mailDeliveryOption: <P>
mailForwarding: <0>
mailImapAccess: <all>
mailImapSslAccess: <all>
mailInterManager: <1>
mailInterManagerSsl: <1>
mailLdapAccess: <all>
mailMtaFilter: <0>
mailMtaFilterPerUser: <0>
mailParentalControl: <1>
mailPopAccess: <all>
mailPopSslAccess: <all>
mailQuotaBounceNotify: <1>
mailQuotaMaxMsgKB: <100>
mailQuotaMaxMsgs: <1000>
mailQuotaThreshold: <70>
mailQuotaTotKb: <10000>
mailSelfCare: <1>
mailSelfCareSsl: <1>
mailSmtAccess: <1>
mailSmtAuth: <0>
mailSmtSslAccess: <1>
mailWebmailAccess: <1>
mailWebmailUseSignature:<1>
```

Are the mail user preference attributes that define the services enabled for the default class of service, which has full administrative permission. For the definitions and possible values of these attributes, see Chapter 7.

```
<list of
adminAttributeConstraint
attributes>
```

Is a list of attributes that specify who can modify specific class-of-service attributes for an account. For more information, see “Adding Attribute Constraints” on page 92.

```
description: <text
description of this
administrative policy>
```

Is a text description of the new administrative policy.

2. Save this LDIF file.

Use the `ldapadd` command to add the new administrative policy:

```
ldapadd -D <binddn> -w <password> -f <filename>
```

Where:

- D <binddn> Uses <binddn> to bind to the directory. <binddn> should be a DN as defined in RFC 1779.
- w <password> Uses <password> as the password for simple authentication
- f <filename> Specifies the name of the LDIF file you just created as the source of a new entry in the Directory database.

Adding Attribute Constraints

The `adminAttributeConstraint` attributes of the `adminPolicy` structural object class specify who can modify specific class-of-service attributes for an account. Class-of-service attributes control access permissions, mailbox quotas, and user preferences, and are found in the `mailUserPrefs` auxiliary object class. For definitions and syntaxes of these object classes and attributes, see Chapter 7.

You add a new attribute constraint to an existing class-of-service (called `full` in this example) when you want to define a new set of access permissions for a user or group of users. You do this using the `ldapmodify` utility.

To add a new attribute constraint:

1. Create an LDIF file to add the new attribute constraint:

```
dn: cn=full, cn=admin root
changeType: modify
add: adminAttributeConstraint
adminAttributeConstraint:1,<access-level>,<attribute-
name>,<constraint>,<value>
```

Where:

1	Is the version number to keep track of changes.
<access-level>	Is the access level an administrator must have to modify the value of an attribute. Access levels are listed in the table on page 98.
<attribute-name>	Is the name of the attribute to be constrained.
<constraint>	Is one of the following: MODIFY, meaning the value may be modified NO_MODIFY, meaning the value may not be modified RANGE, meaning the value must be within the specified range CHOICE, meaning the value is one of the specified choices
<value>	Specifies the choices for the CHOICE option. Specifies a range of values for the RANGE option.

2. Save this LDIF file.
3. Use the `ldapmodify` command to add the new constraint:

```
ldapmodify -D <binddn> -w <password> -f <filename>
```

Where:

-D <binddn>	Uses <binddn> to bind to the directory. <binddn> should be a DN as defined in RFC 1779.
-------------	---

<code>-w <password></code>	Uses <code><password></code> as the password for simple authentication
<code>-f <filename></code>	Specifies the name of the LDIF file you just created as the source of a new entry in the Directory database.

There are a number of default access constraints in the `init_dit.ldif` file. For example, the following constraint specifies that an authenticated user with no administrative permission (access level 10) is not allowed to modify the flag enabling access to the standard SMTP service:

```
adminAttributeConstraint: <1,10,mailSmtAccess,NO_MODIFY>
```

The following constraint specifies that a Group Administrator (access level 100) has the authority to enable or disable account access to the SMTP service:

```
adminAttributeConstraint: <1,100,mailSmtAccess,CHOICE,0,1>
```

The following constraint specifies that a Group Administrator has the authority to control account access to the SSL-encrypted IMAP service:

```
adminAttributeConstraint: <1,100,mailImapSslAccess,CHOICE,all,
trusted,none>
```

The `adminAttributeConstraint` attribute also defines the range of mail quota values for the number of messages that can be accepted in an account's mailbox, the maximum size of a message, the maximum total storage space for messages, and the point at which a warning to delete some messages appears. For example, the following constraint specifies that a Group Administrator has the authority to set the maximum size of a message that can be accepted into an account's mailbox at any level between 0 and 100 kilobytes:

```
adminAttributeConstraint: <1,100,mailQuotaMaxMsgKB,RANGE,0-100>
```

Modifying Attribute Constraints

Administrators with permission to modify attribute constraints can give permission to lower level administrators to modify specific class-of-service attributes.

To modify an existing attribute constraint in an administrative policy:

1. Create an LDIF file to modify the attribute constraint:

```
dn: cn=roleSPA, cn=admin root
changeType: modify
delete: adminAttributeConstraint
adminAttributeConstraint: <version>,
<access-level>, <attribute-name>, <constraint>, <old_value>
-
add: adminAttributeConstraint
adminAttributeConstraint: <version,access-level,
attribute-name,constraint,new_value>
```

Where:

<code>dn: cn=roleSPA, cn=admin root</code>	Is the distinguished name of the administrative role whose permissions you are modifying.
<code>changeType: modify</code>	Indicates that you are modifying an entry.
<code>delete: adminAttributeConstraint</code>	Indicates that you are deleting an <code>adminAttributeConstraint</code> attribute.
<code>adminAttributeConstraint: <version,access-level,attribute-name,constraint,old_value></code>	Is the old value of the <code>adminAttributeConstraint</code> attribute that you want to delete.
<code>-</code>	Is a separator between operations.
<code>add: adminAttributeConstraint</code>	Indicates that you are adding an <code>adminAttributeConstraint</code> attribute.
<code>adminAttributeConstraint: <version,access-level,attribute-name,constraint,new_value></code>	Is the new value of the <code>adminAttributeConstraint</code> attribute that you want to add.

2. Save this LDIF file.
3. Use the `ldapmodify` command to modify the attribute constraint value:

```
ldapmodify -D <binddn> -w <password> -f <filename>
```

Where:

<code>-D <binddn></code>	Uses <code><binddn></code> to bind to the directory. <code><binddn></code> should be a DN as defined in RFC 1779.
<code>-w <password></code>	Uses <code><password></code> as the password for simple authentication.
<code>-f <filename></code>	Specifies the name of the LDIF file you just created as the source of a new entry in the Directory database.

Modifying Class-of-Service Attributes

The default values of the class-of-service attributes for the highest class of service (called `full` because it has the full set of access privileges) are initialized in the `init_dit.ldif` file. The definitions and possible values of these attributes are described in Chapter 7.

You modify class-of-service attribute values when you want to change the permissions or the mail user preferences for a class-of-service.

To modify class-of-service attribute values:

1. Create an LDIF file to define the attribute values to be modified:

```
dn: cn=full, cn=admin root
changeType: modify
delete: <attributeName>
<attributeName>: <old_value>
-
add: <attributeName>
<attributeName>: <new_value>
```

Where:

dn: cn=full, cn=admin root	Is the distinguished name of the administrative policy called <code>full</code> .
changeType: modify	Indicates that you are modifying the entry.
delete: <attributeName>	Indicates that you are deleting the value of an attribute.
<attributeName>: <old_value>	Is the value of the attribute that you are deleting.
-	Is a separator between operations.
add: <attributeName>	Indicates that you are adding the value of an attribute.
<attributeName>: <new_value>	Is the value of the attribute that you are adding.

2. Save this LDIF file.
3. Use the `ldapmodify` command to modify the attribute values:

```
ldapmodify -D <binddn> -w <password> -f <filename>
```

Where:

-D <binddn>	Uses <binddn> to bind to the directory. <binddn> should be a DN as defined in RFC 1779.
-w <password>	Uses <password> as the password for simple authentication.
-f <filename>	Specifies the name of the LDIF file you just created as the source of a new entry in the Directory database.

Adding COS Attributes

Adding a new COS attribute requires making a change to the Directory schema. The `mailUserPrefs` object class contains pre-defined class of service related mail attributes that specify user preferences for POP, IMAP, WebEdge, and SMTP access. The `mailLocalUserPrefs` object class is defined to contain any custom mail attributes that you wish to create for your organization. For information on how to do this, see Chapter 5.

Adding Allocation Rules

The initial DIT defines allocation rules that specify attributes to be counted, such as the total number of accounts, the number of accounts able to use a certain feature, the number of domains, and so on. These rules take the following form:

```
adminAllocRules:
1, <attributeName>, <numAttribute>, <maxAttribute>, <valuecount=#>
```

Where:

1	Is the version number, which is used to keep track of rule changes.
attributeName	Is the name of an attribute used in the application tree entry.
numAttribute	Is the name of the attribute in the <code>adminAllocation</code> object class that specifies the current number of the thing you are counting.
maxAttribute	Is the name of an attribute in the <code>adminAllocation</code> object class that specifies the maximum number of the thing you are counting.
valuecount=#	Is a list of values and their counts. <i>Note: For Boolean attributes, the syntax is:</i> <i>*=boolean</i> <i>where * is equal to 1 if True, and equal to 0 if False.</i> <i>For integer attributes, the syntax is:</i> <i>*=integer</i> <i>where * is the integer value.</i>

To add a new allocation rule:

1. Create an LDIF file to add the new allocation rule:

```
dn: cn=admin root
changeType: modify
add: adminAllocRules
adminAllocRules: 1, <newAttribute>, <numAttribute>,
<maxAttribute>, <valueCount=1>
```

Where:

<code>dn: cn=admin root</code>	Is the distinguished name of the structural root of the administration tree.
<code>changeType: modify</code>	Indicates that you are modifying a schema entry.
<code>add: adminAllocRules</code>	Indicates that you are adding an allocation rule.
<code>adminAllocRules: <1, newAttribute, numAttribute, maxAttribute, valueCount=1></code>	Defines the new allocation rule.

2. Save this LDIF file.
3. Use the `ldapmodify` command to add the new allocation rule:

```
ldapmodify -D <binddn> -w <password> -f <filename>
```

Where:

<code>-D <binddn></code>	Uses <code><binddn></code> to bind to the directory. <code><binddn></code> should be a DN as defined in RFC 1779.
<code>-w <password></code>	Uses <code><password></code> as the password for simple authentication.
<code>-f <filename></code>	Specifies the name of the LDIF file you just created as the source of a new entry in the Directory database.

Note: You must also modify the Directory schema object class `adminAllocation` to add the new attributes `numAttribute` and `maxAttribute`. For instructions for adding attributes to the Directory schema, see Chapter 5.

Defining Administrative Roles

InterMail's initial DIT specifies the access control privileges for several InterMail administrative roles. The `accessLevel` attribute in the `adminRole` entry numerically represents the access level of a role in the DIT in order to show the role hierarchy. Roles with higher access levels have more privileges to create and modify Directory database entries than do roles with lower access levels. Members of each role can create and delete administrative groups with lower access levels.

Note: You should not modify the access level of a role.

The predefined administrative roles and their access levels are:

Role	Access Level
Supervisory Provider Administrator (SPA)	900
Provider Administrator (PA)	800
Supervisory Customer Service Representative (SCSR)	700
Customer Service Representative (CSR)	600
Supervisory Organization Administrator (SOA)	500
Organization Administrator (OA)	400
Organizational Unit Administrator (OUA)	300
Group Administrator (GA)	100
Head of Household (HOH)	50
Authenticated User (no administrative permission)	10
Anonymous Login (non-authenticated user)	1

Note: If you log in as `root`, you bypass all attribute constraint checks and have permission to change any directory data. Use `root` access only if the task cannot be performed by any of the other roles.

Adding Administrative Realms

We recommend that you use the InterManager GUI if you wish to add a new `adminRealm`.

7

Directory Schema Tables

The Integrated Services Directory (ISD) schema defines the rules for the structure and values of the data that can be stored in the Directory database and the Directory Cache databases. It sets the rules that the Directory server and its clients use during account provisioning and during search and update operations. All servers and utilities read the schema from the `schema.ldif` file, whose pathname is specified in the Configuration database on each host machine. The Directory server and the Directory Cache servers write the schema as an entry in their databases.

In LDAP-based directories such as the ISD, the schema is composed of attribute and object class definitions. An attribute is information describing one trait of a Directory database object. An object class is a collection of attributes that defines a type of data. For example, a user's common name, surname, and password are represented by the `cn`, `sn`, and `userName` attributes in the `person` object class. For a detailed explanation of object classes and attributes, see Chapter 5.

The ISD schema is extensible; that is, you can add attributes and object classes to it in order to meet the unique needs of your organization. For instructions on how to customize the schema, see Chapter 5.

This chapter defines the LDAP object classes and attributes in the ISD schema. It presents this information in two types of tables:

- Tables defining object classes
- Tables defining attributes, which are listed alphabetically

Note: The ISD schema is subject to change without notice by Software.com. Never make changes to the Directory database directly. Instead, use the `ldapadd` and `ldapmodify` utilities to customize the schema. For instructions on how to do this, see Chapter 5. For a discussion of the APIs, see the *InterMail Mx Reference Guide*.

Tables Defining LDAP Object Classes

An object class is defined in the ISD schema by:

- A name that uniquely identifies the object class
- An object identifier (OID)
- A class type (structural, auxiliary, or abstract)
- Mandatory attributes
- Optional attributes

For example, the InterMail auxiliary object class `mailDomain` is defined in the `schema.ldif` file as follows:

```
objectclasses: (1.3.6.1.4.1.2415.2.2.2.2
NAME 'mailDomain'
SUP top AUXILIARY
MUST ( domainName $ domainType )
MAY ( mailRelayHost $ mailRewriteDomain $ mailWildcardAccount ) )
```

Where:

<code>objectclasses</code>	Indicates that an object class is defined.
<code>1.3.6.1.4.1.2415.2.2.2.2</code>	Is the OID. <i>Note:</i> You can request OIDs for your organization from the Internet Assigned Numbers Authority (IANA), using the form at URL http://www.isi.edu/cgi-bin/iana/enterprise.pl
<code>NAME 'mailDomain'</code>	Defines the name of the object class as <code>mailDomain</code> .
<code>SUP top</code>	Indicates that the parent object class of <code>mailDomain</code> is <code>top</code> .
<code>AUXILIARY</code>	Defines <code>mailDomain</code> as an auxiliary object class.
<code>MUST (domainName \$ domainType)</code>	Lists the mandatory attributes of the <code>mailDomain</code> object class, separated by <code>\$</code> .
<code>MAY (mailRelayHost \$ mailRewriteDomain \$ mailWildcardAccount)</code>	Lists the optional attributes of the <code>mailDomain</code> object class, separated by <code>\$</code> .

This section alphabetically lists and defines each of the object classes in InterMail. The mandatory attributes within each object class are listed alphabetically in a table, followed by an alphabetical list of the optional attributes. LDAP standard object

classes and attributes are noted by a reference to the RFC and paragraph number in which they are defined, for example, RFC 2256 paragraph 5.4. You can find the RFCs at <http://www.rfc-editor.org>.

adminAllocation

Class Type: auxiliary

Parent Class: top

Related Structural Classes: adminRealm, adminAllocCounts

This object class is used to set numerical limits for licensed or allocated features used within an adminRealm object, such as number of users, storage space, number of organizations, number of accounts with POP service enabled, number of accounts with IMAP service enabled, and number of accounts with WebEdge enabled.

Attributes have prefixes of max, num, or used. max indicates the upper limit, while num and used indicate the amount currently used. When a mailUser object is created or updated, the currently-used attributes for the newly enabled features for that account are incremented from the corresponding adminAllocation object. When features are disabled, the corresponding currently-used attributes of adminAllocation are decremented. If the feature enabled causes the allocation to reach its maximum limit, the update is denied.

Attribute Name	Mandatory/Optional
adminAllocSubtots	Optional
adminMaxDomains	Optional
adminMaxIMAP	Optional
adminMaxIMAPSSL	Optional
adminMaxInterManager	Optional
adminMaxMailingLists	Optional
adminMaxPOP	Optional
adminMaxPOPSSL	Optional
adminMaxRealms	Optional
adminMaxSelfCare	Optional
adminMaxSMTP	Optional
adminMaxSMTPSSL	Optional

Attribute Name	Mandatory/Optional
adminMaxStorageKB	Optional
adminMaxUsers	Optional
adminMaxWebMail	Optional
adminNumDomains	Optional
adminNumIMAP	Optional
adminNumIMAPSSL	Optional
adminNumInterManager	Optional
adminNumMailingLists	Optional
adminNumPOP	Optional
adminNumPOPSSL	Optional
adminNumRealms	Optional
adminNumSelfCare	Optional
adminNumSMTP	Optional
adminNumSMTPSSL	Optional
adminNumUsers	Optional
adminNumWebMail	Optional
adminPolicyDNUsed	Optional
adminUsedStorageKB	Optional

adminAllocCounts

Class Type: structural

Parent Class: `top`

This object class is used internally for tracking allocations.

Attribute Name	Mandatory/Optional
cn	Mandatory

adminGroup

Class Type: structural

Parent Class: groupOfNames

This object class defines the permissions associated with a group of administrators. The `member` attribute of the `groupOfNames` class identifies the person entries of the group.

Attribute Name	Mandatory/Optional
adminRoleDN	Mandatory
adminAllowedAdminPolicyDN	Optional
adminAllowedDomains	Optional
adminAttributeConstraint	Optional
adminParentDomains	Optional
adminSuperiorAttributeConstraint	Optional
contactInfo	Optional
member	Optional

adminPolicy

Class Type: structural

Parent Class: top

Auxiliary Classes: mailLocalUserPrefs, mailUserPrefs

This object class represents a class-of-service, and contains attribute values representing the mail policy for an end-user.

The `adminAttributeConstraint` attribute defines the rules governing who may change an `adminPolicy` attribute and what values those attributes may be assigned.

Classes of service are described in the *InterMail Mx Operations Guide*.

Attribute Name	Mandatory/Optional
cn	Mandatory
adminAttributeConstraint	Optional
adminParentAdminPolicy	Optional

Attribute Name	Mandatory/Optional
adminProvisionOnly	Optional
adminTemplateOnly	Optional
description	Optional

adminRealm

Class Type: structural

Parent Class: top

Auxiliary Classes: adminAllocation

This object class is the basic building block of administrative control in the Integrated Services Directory (ISD). Objects in this class are created and maintained through the InterManager GUI. The Directory server enforces the access privileges described.

The adminGroup objects directly beneath an adminRealm object define groups of people with administrative privileges within the scope of the adminRealm object.

Attribute Name	Mandatory/Optional
cn	Mandatory
adminApprovedSendersList	Optional
adminAttributeConstraint	Optional
adminParentalRejectAction	Optional
adminPolicyGrantDN	Optional
adminSuperiorAttributeConstraint	Optional
adminTargetDN	Optional
billingId	Optional
contactInfo	Optional

adminRealmSpec

Class Type: structural

Parent Class: top

This object class contains the default values for realm related entries. It provides a template for realm creation in the InterManager GUI.

Attribute Name	Mandatory/Optional
adminRealmType	Mandatory
adminDefaultCreatedGroups	Optional
adminDomainSpecControl	Optional
adminMinAllowedAccessLevel	Optional
adminTargetObjectClass	Optional

adminRole

Class Type: structural

Parent Class: top

Auxiliary Classes: none

This object class defines the access control privileges for associated InterMail administrative groups. These objects are defined in the Configuration database (config.db) and are read-only on the server.

Attribute Name	Mandatory/Optional
adminAccessLevel	Mandatory
cn	Mandatory
adminAllowedCreateClasses	Optional
adminAllowedUpdateClasses	Optional
adminCreatePeerAdminGroup	Optional
adminCreatePeerAdminPolicy	Optional
adminCreateRealm	Optional
adminCreateSubAdminGroup	Optional

Attribute Name	Mandatory/Optional
adminCreateSubAdminPolicy	Optional
adminDefinePeerAdminPolicyAttribute	Optional
adminDefineSubAdminPolicyAttribute	Optional
adminDeletePeerAdminGroup	Optional
adminDeletePeerAdminPolicy	Optional
adminDeleteRealm	Optional
adminDeleteSubAdminGroup	Optional
adminDeleteSubAdminPolicy	Optional

adminRoot

Class Type: structural

Parent Class: top

This object class is the structural root of the administration tree, containing policies, roles, realms, and administrative groups.

Attribute Name	Mandatory/Optional
cn	Mandatory
adminAllocationRules	Optional
adminPolicyDefaultDN	Optional

adminTarget

Class Type: auxiliary

Parent Class: top

Related Structural Classes: domain, inetOrgPerson, organization, organizationalUnit

This object class is mixed with each of the InterMail structural object classes in the application tree of the DIT in order to identify the realm associated with each.

Attribute Name	Mandatory/Optional
adminRealmDN	Mandatory

adminUserPrefs

Class Type: auxiliary

Parent Class: top

Related Structural Class: inetOrgPerson, person

This object class can be mixed in with any `inetOrgPerson`. It specifies additional attributes that can be used by the InterManager GUI.

Attribute Name	Mandatory/Optional
adminLastLogin	Optional
adminPreferredLocale	Optional
labeledURI	Optional

alias

Class Type: structural

Parent Class: top

This is an LDAP standard object class, defined in RFC 2256 paragraph 7.2.

Attribute Name	Mandatory/Optional
aliasedObjectName	Mandatory

applicationEntity

Class Type: structural

Parent Class: top

This is an LDAP standard object class, defined in RFC 2256 paragraph 7.13.

Attribute Name	Mandatory/Optional
presentationAddress	Mandatory
cn	Mandatory
description	Optional
l	Optional
o	Optional
ou	Optional

Attribute Name	Mandatory/Optional
seeAlso	Optional
supportedApplicationContext	Optional

applicationProcess

Class Type: structural

Parent Class: `top`

This is an LDAP standard object class, defined in RFC 2256 paragraph 7.12.

Attribute Name	Mandatory/Optional
cn	Mandatory
description	Optional
l	Optional
ou	Optional
seeAlso	Optional

certificationAuthority

Class Type: auxiliary

Parent Class: `top`

This is an LDAP standard object class, defined in RFC 2256 paragraph 7.17.

Attribute Name	Mandatory/Optional
authorityRevocationList	Mandatory
cACertificate	Mandatory
certificateRevocationList	Mandatory
crossCertificatePair	Optional

certificationAuthority-V2

Class Type: auxiliary

Parent Class: certificationAuthority

This is an LDAP standard object class, defined in RFC 2256 paragraph 7.20.

Attribute Name	Mandatory/Optional
deltaRevocationList	Optional

changeLogEntry

Class Type: structural

Parent Class: top

Auxiliary Classes: none

This object class is used to store LDAP change logs in the Directory database.

This is an LDAP standard object class, described in draft-good-ldap-changelog-00.txt.

Attribute Name	Mandatory/Optional
changeNumber	Mandatory
changeType	Mandatory
targetDN	Mandatory
changes	Optional
deleteOldRDN	Optional
newRDN	Optional
newSuperior	Optional

country

Class Type: structural

Parent Class: top

This is an LDAP standard object class, defined in RFC 2256 paragraph 7.3.

Attribute Name	Mandatory/Optional
c	Mandatory

Attribute Name	Mandatory/Optional
description	Optional
enhancedSearchGuide	Optional

cRLDistributionPoint

Class Type: structural

Parent Class: top

This is an LDAP standard object class, defined in RFC 2256 paragraph 7.21.

Attribute Name	Mandatory/Optional
cn	Mandatory
authorityRevocationList	Optional
certificateRevocationList	Optional
deltaRevocationList	Optional

dcObject

Class Type: auxiliary

Parent Class: top

Related Structural Classes: organization, organizationalUnit

This is an LDAP standard object class (RFC 2247 paragraph 5.1) that identifies domain component objects.

Attribute Name	Mandatory/Optional
dc	Mandatory

device

Class Type: structural

Parent Class: top

This is an LDAP standard object class, defined in RFC 2256 paragraph 7.15.

Attribute Name	Mandatory/Optional
cn	Mandatory

Attribute Name	Mandatory/Optional
description	Optional
l	Optional
o	Optional
ou	Optional
owner	Optional
seeAlso	Optional
serialNumber	Optional

dmd

Class Type: structural

Parent Class: top

This is an LDAP standard object class, defined in RFC 2256 paragraph 7.22.

Attribute Name	Mandatory/Optional
dmdName	Mandatory
businessCategory	Optional
description	Optional
destinationIndicator	Optional
enhancedSearchGuide	Optional
facsimileTelephoneNumber	Optional
internationalISDNNumber	Optional
l	Optional
physicalDeliveryOfficeName	Optional
postalAddress	Optional
postalCode	Optional
postOfficeBox	Optional

Attribute Name	Mandatory/Optional
preferredDeliveryMethod	Optional
registeredAddress	Optional
seeAlso	Optional
st	Optional
street	Optional
telephoneNumber	Optional
teletexTerminalIdentifier	Optional
telexNumber	Optional
userPassword	Optional
x121Address	Optional

domain

Class Type: structural

Parent Class: top

Auxiliary Classes: adminTarget, mailDomain

This is an LDAP standard object class (RFC 2247 paragraph 5.2) that identifies the owner of a network address. The domain name of an account is included in its primary e-mail address. For example, *software.com* is a domain name.

Attribute Name	Mandatory/Optional
dc	Mandatory
businessCategory	Optional
description	Optional
destinationIndicator	Optional
enhancedSearchGuide	Optional
facsimileTelephoneNumber	Optional
internationalISDNNumber	Optional

Attribute Name	Mandatory/Optional
l	Optional
o	Optional
physicalDeliveryOfficeName	Optional
postalAddress	Optional
postalCode	Optional
postalOfficeBox	Optional
preferredDeliveryMethod	Optional
registeredAddress	Optional
seeAlso	Optional
st	Optional
street	Optional
telephoneNumber	Optional
teletexTerminalIdentifier	Optional
telexNumber	Optional
userPassword	Optional
x121Address	Optional

dsA

Class Type: structural

Parent Class: applicationEntity

This is an LDAP standard object class defined in RFC 2256 paragraph 7.14.

Attribute Name	Mandatory/Optional
knowledgeInformation	Optional

groupOfNames

Class Type: structural

Parent Class: top

Auxiliary Classes: none

This is an LDAP standard object class (RFC 2256 paragraph 7.10) that specifies the names of members in an administrative group.

Attribute Name	Mandatory/Optional
cn	Mandatory
businessCategory	Optional
description	Optional
member	Optional
o	Optional
ou	Optional
owner	Optional
seeAlso	Optional

groupOfUniqueNames

Class Type: structural

Parent Class: top

This is an LDAP standard object class defined in RFC 2256 paragraph 7.18.

Attribute Name	Mandatory/Optional
cn	Mandatory
uniqueMember	Mandatory
businessCategory	Optional
description	Optional
o	Optional
ou	Optional
owner	Optional

Attribute Name	Mandatory/Optional
seeAlso	Optional

inetOrgPerson

Class Type: structural

Parent Class: organizationalPerson

Auxiliary Classes: adminTarget, adminUserPrefs, mailLocalUserPrefs, mailUser, mailUserPrefs

This is an LDAP standard object class (Internet Draft <http://search.ietf.org/internet-drafts/draft-smith-ldap-inetorgperson-03.txt>) that represents people who are associated with an organization.

Attribute Name	Mandatory/Optional
audio	Optional
businessCategory	Optional
carLicense	Optional
departmentNumber	Optional
displayName	Optional
employeeNumber	Optional
employeeType	Optional
givenName	Optional
homePhone	Optional
homePostalAddress	Optional
initials	Optional
jpegPhoto	Optional
labeledURI	Optional
mail	Optional
manager	Optional
mobile	Optional

Attribute Name	Mandatory/Optional
o	Optional
pager	Optional
photo	Optional
preferredLanguage	Optional
roomNumber	Optional
secretary	Optional
uid	Optional
userCertificate	Optional
userPKCS12	Optional
userSMIMECertificate	Optional
x500UniqueIdentifier	Optional

locality

Class Type: structural

Parent Class: `top`

This is an LDAP standard object class, defined in RFC 2256 paragraph 7.4.

Attribute Name	Mandatory/Optional
description	Optional
enhancedSearchGuide	Optional
l	Optional
seeAlso	Optional
st	Optional
street	Optional

mailDomain

Class Type: auxiliary

Parent Class: top

Related Structural Classes: domain

This object class specifies a DNS domain name for InterMail e-mail addresses and related attributes. It is used to add mail-related attributes to domain entries.

Attribute Name	Mandatory/Optional
domainName	Mandatory
domainType	Mandatory
mailRelayHost	Optional
mailRewriteDomain	Optional
mailWildcardAccount	Optional

mailLocalUserPrefs

Class Type: auxiliary

Parent Class: top

Related Structural Classes: adminPolicy, inetOrgPerson

This object class is for extended attributes only; it is delivered empty. Customers define new class-of-service attributes and user preferences here. These custom attributes are treated just like the attributes in mailUserPrefs.

mailUser

Class Type: auxiliary

Parent Class: top

Related Structural Classes: inetOrgPerson

This object class adds mail-related attributes to the person object class. It can be mixed with object classes, such as residentialPerson, organizationalPerson, and so on.

Attribute Name	Mandatory/Optional
adminPolicyDN	Mandatory
mail	Mandatory

Attribute Name	Mandatory/Optional
billingId	Optional
mailAlternateAddress	Optional
mailAutoReplyHost	Optional
mailboxId	Optional
mailboxStatus	Optional
mailForwardingAddress	Optional
mailLogin	Optional
mailMessageStore	Optional
mailPassword	Optional
mailPasswordType	Optional
mailPOPProxyHost	Optional
mailSMTPRelayHost	Optional

mailUserPrefs

Class Type: auxiliary

Parent Class: top

Related Structural Classes: adminPolicy, inetOrgPerson

This object class contains class-of-service-related mail attributes, including permissions for POP, IMAP, WebEdge, and SMTP access.

Attribute Name	Mandatory/Optional
mailAllowTheseIps	Optional
mailAutoReplyMode	Optional
mailBypassAuthentication	Optional
mailDeliveryOption	Optional
mailForwarding	Optional
mailIMAPAccess	Optional

Attribute Name	Mandatory/Optional
mailIMAPSSLAccess	Optional
mailInterManager	Optional
mailInterManagerSSL	Optional
mailLdapAccess	Optional
mailMTAFilter	Optional
mailMTAFilterPerUser	Optional
mailParentalControl	Optional
mailPOPAccess	Optional
mailPOPSSLAccess	Optional
mailQuotaBounceNotify	Optional
mailQuotaMaxMsgKB	Optional
mailQuotaMaxMsgs	Optional
mailQuotaThreshold	Optional
mailQuotaTotKB	Optional
mailSelfCare	Optional
mailSelfCareSSL	Optional
mailSMTPAccess	Optional
mailSMTPAuth	Optional
mailSMTPSSLAccess	Optional
mailWebMailAccess	Optional
mailWebMailAddressBookLimit	Optional
mailWebMailAddressBookListLimit	Optional
mailWebMailAttachLimit	Optional
mailWebMailAttachSizeLimit	Optional

Attribute Name	Mandatory/Optional
mailWebMailConfirmDelete	Optional
mailWebMailMsgAttachLimit	Optional
mailWebMailUseSignature	Optional

organization

Class Type: structural

Parent Class: top

Auxiliary Classes: adminTarget, dcObject

This is an LDAP standard object class (RFC 2256 paragraph 7.5) that corresponds to an entire company or other top-level institution. Organizations are typically created when a company initially purchases an initial set of e-mail accounts and services. Organizations are containers for organizational units and e-mail accounts.

Attribute Name	Mandatory/Optional
o	Mandatory
businessCategory	Optional
description	Optional
destinationIndicator	Optional
enhancedSearchGuide	Optional
facsimileTelephoneNumber	Optional
internationalISDNNumber	Optional
l	Optional
physicalDeliveryOfficeName	Optional
postalAddress	Optional
postalCode	Optional
postOfficeBox	Optional
preferredDeliveryMethod	Optional
registeredAddress	Optional

Attribute Name	Mandatory/Optional
seeAlso	Optional
st	Optional
street	Optional
telephoneNumber	Optional
teletexTerminalIdentifier	Optional
telexNumber	Optional
userPassword	Optional
x121Address	Optional

organizationalPerson

Class Type: structural

Parent Class: person

Auxiliary Classes: none

This is an LDAP standard object class (RFC 2256 paragraph 7.8) that describes an employee within an organization.

Attribute Name	Mandatory/Optional
destinationIndicator	Optional
facsimileTelephoneNumber	Optional
internationalISDNNumber	Optional
l	Optional
ou	Optional
physicalDeliveryOfficeName	Optional
postalAddress	Optional
postalCode	Optional
postalOfficeBox	Optional
preferredDeliveryMethod	Optional

Attribute Name	Mandatory/Optional
registeredAddress	Optional
st	Optional
street	Optional
telephoneNumber	Optional
teletexTerminalIdentifier	Optional
telexNumber	Optional
title	Optional
x121Address	Optional

organizationalRole

Class Type: structural

Parent Class: top

This is an LDAP standard object class, defined in RFC 2256 paragraph 7.9.

Attribute Name	Mandatory/Optional
cn	Mandatory
description	Optional
destinationIndicator	Optional
facsimileTelephoneNumber	Optional
internationalISDNNumber	Optional
l	Optional
ou	Optional
physicalDeliveryOfficeName	Optional
postalAddress	Optional
postalCode	Optional
postOfficeBox	Optional

Attribute Name	Mandatory/Optional
preferredDeliveryMethod	Optional
registeredAddress	Optional
roleOccupant	Optional
seeAlso	Optional
st	Optional
street	Optional
telephoneNumber	Optional
teletexTerminalIdentifier	Optional
telexNumber	Optional
x121Address	Optional

organizationalUnit

Class Type: structural

Parent Class: top

Auxiliary Classes: adminTarget, dcObject

This is an LDAP standard object class (RFC 2256 paragraph 7.6) that identifies a group within an organization, such as a department within a company. This object class is used as a convenience for subdividing an organization and is optional.

Attribute Name	Mandatory/Optional
ou	Mandatory
businessCategory	Optional
description	Optional
destinationIndicator	Optional
enhancedSearchGuide	Optional
facsimileTelephoneNumber	Optional
internationalISDNNumber	Optional

Attribute Name	Mandatory/Optional
l	Optional
physicalDeliveryOfficeName	Optional
postalAddress	Optional
postalCode	Optional
postOfficeBox	Optional
preferredDeliveryMethod	Optional
registeredAddress	Optional
seeAlso	Optional
st	Optional
street	Optional
telephoneNumber	Optional
teletexTerminalIdentifier	Optional
telexNumber	Optional
userPassword	Optional
x121Address	Optional

partition

Class Type: structural

Parent Class: top

Auxiliary Classes: none

This object class is used internally to define partitions in the Configuration database.

Attribute Name	Mandatory/Optional
cn	Mandatory
partition	Optional

person

Class Type: structural

Parent Class: top

Auxiliary Classes: adminTarget, mailUser, mailUserPrefs, mailLocalUserPrefs

This is an LDAP standard object class (RFC 2256 paragraph 7.7) that corresponds to an individual user within an organizational unit. A person object specifies information such as a person's name, password, and telephone number.

Attribute Name	Mandatory/Optional
cn	Mandatory
sn	Mandatory
description	Optional
seeAlso	Optional
telephoneNumber	Optional
userPassword	Optional

replAgreement

Class Type: structural

Parent Class: top

Auxiliary Classes: none

This object class is used internally to store replication agreements defined in the Configuration database.

Attribute Name	Mandatory/Optional
cn	Mandatory
updateInterval	Mandatory
consumerIdentity	Optional
consumerPassword	Optional
lastChangeNumber	Optional
replArea	Optional

Attribute Name	Mandatory/Optional
supplierReference	Optional

residentialPerson

Class Type: structural

Parent Class: person

This is an LDAP standard object class, defined in RFC 2256 paragraph 7.11.

Attribute Name	Mandatory/Optional
1	Mandatory
businessCategory	Optional
destinationIndicator	Optional
facsimileTelephoneNumber	Optional
internationalISDNNumber	Optional
physicalDeliveryOfficeName	Optional
postalAddress	Optional
postalCode	Optional
postOfficeBox	Optional
preferredDeliveryMethod	Optional
registeredAddress	Optional
st	Optional
street	Optional
telephoneNumber	Optional
teletexTerminalIdentifier	Optional
telexNumber	Optional
x121Address	Optional

scConfig

Class Type: structural

Parent Class: top

This object class represents a configuration object.

Attribute Name	Mandatory/Optional
cn	Mandatory
scAttributeIndexInfo	Optional

scConfigRoot

Class Type: structural

Parent Class: top

This object class represents the configuration root.

Attribute Name	Mandatory/Optional
cn	Mandatory
scCacheDirDbStatus	Optional

subschema

Class Type: auxiliary

This object class is used to store the LDAP schema in the Directory database. It is defined in RFC 2252 paragraph 7.2.

Attribute Name	Mandatory/Optional
attributeTypes	Optional
ditContentRules	Optional
ditStructureRules	Optional
matchingRules	Optional
matchingRuleUse	Optional
nameForms	Optional
objectClasses	Optional

top

Class Type: abstract

This is an LDAP standard super object class (RFC 2256 paragraph 7.1) from which all structural object classes are derived. This object class ensures that all LDAP entries contain an `objectClass` value.

Attribute Name	Mandatory/Optional
<code>objectClass</code>	Mandatory

userSecurityInformation

Class Type: auxiliary

Parent Class: `top`

This is an LDAP standard object class, defined in RFC 2256 paragraph 7.19.

Attribute Name	Mandatory/Optional
<code>supportedAlgorithms</code>	Optional

Tables Defining LDAP Attributes

An attribute is defined in the ISD schema by:

- A name that uniquely identifies the attribute
- An OID
- A matching rule
- A syntax type
- An indication of whether the attribute can have only a single value or multiple values
- Constraints on the attribute values

For example, the `schema.ldif` file defines the attribute `domainType` as follows:

```
attributetypes: ( 1.3.6.1.4.1.2415.2.2.1.5
NAME 'domainType'
EQUALITY caseExactMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.44 {1} SINGLE-VALUE
X-VALUE-CONSTRAINT 'CHOICE,L,R,N,I' )
```

Where:

`attributetypes`

Indicates that an attribute is defined.

1.3.6.1.4.1.2415.2.2.1.5	Is the OID. <i>Note:</i> You can request OIDs for your organization from the Internet Assigned Numbers Authority (IANA), using the form at this URL: http://www.isi.edu/cgi-bin/iana/enterprise.pl
NAME 'domainType'	Defines the name of the attribute as domainType.
EQUALITY caseExactMatch	Defines the matching rule for this attribute as caseExactMatch, meaning that uppercase and lowercase letters are deemed different. <i>Note:</i> For a list of matching rules used in equality filters, see section 8 of RFC 2252, LDAP v3 Attribute Syntax Definitions. The URL is: http://www.rfc-editor.org/rfcsearch.html
SYNTAX 1.3.6.1.4.1.1466.115.121.1.44	Defines the syntax of this attribute as Printable String. <i>Note:</i> For a list of syntax types and their respective object identifiers, see section 4.3.2 of RFC 2252.
{1}	Constrains the maximum number of characters in the printable string to 1.
SINGLE-VALUE	Constrains the value of this attribute to a single value.
X-VALUE-CONSTRAINT 'CHOICE,L,R,N,I'	Constrains the value of this attribute to one of these single character choices: L, R, N, or I.

This section alphabetically lists and defines each of the attributes associated with the LDAP object classes in the ISD schema, including their values, matching rules, and syntax types.

For the distinguished name syntax type, the description in the following tables may include any of three additional features:

- DN mapping—Indicates that the attribute references other entries. If the distinguished name of any of the referenced entries is changed, the distinguished name of this mapped attribute is automatically changed by the Directory server.
- Attribute indexing—Indicates that the attribute is indexed. You can index attributes that you search for often in order to speed up the search process. For more information on attribute indexing, see Chapter 3.

- Enforcement of referential integrity—Indicates that the entry this attribute references cannot be deleted until the distinguished name reference is removed from the attribute’s value.

For more information on the object classes associated with each attribute, see “Tables Defining LDAP Object Classes” on page 100. For more information on the matching rules and attribute syntaxes used in InterMail, see “Tables Defining LDAP Attributes” on page 128.

Attribute Name	Definition	Object Classes
aciRule	<p>Access control information rule, which specifies who can and cannot read or modify a given directory entry. Each ACI rule has the following components:</p> <ul style="list-style-type: none"> • Identity of the user accessing the data • Directory objects the user can access • Access rights this user has for the specified objects <p>Single or Multiple Value: Multiple Syntax type: Directory String Example: <code>aciRule: cn=John Doe, ou=engineering, self, "", userPassword, entry, ar+aw</code> would allow a user named John Doe to read and change his own password. <i>Note: For more information on ACI rules, see Chapter 2.</i></p>	N/A (Directory operational attribute)
adminAccessLevel	<p>Account access level for members of an administrative group.</p> <p>Single or multiple value: Single Matching rule: integerMatch Syntax type: Integer Default value: 900</p>	adminRole
adminAllocRules	<p>Single or multiple value: Multiple Matching rule: caseIgnoreIA5Match Syntax type: IA5 string</p>	adminRoot
adminAllocSubTots	<p>Single or multiple value: Multiple Matching rule: caseIgnoreIA5Match Syntax type: IA5 string</p>	adminAllocation

Attribute Name	Definition	Object Classes
adminAllowedAdminPolicyDN	<p>List of distinguished names of adminPolicy objects that can be used in creating or updating accounts.</p> <p>Single or multiple value: Multiple</p> <p>Matching rule: distinguishedNameMatch</p> <p>Syntax type: Distinguished name</p>	adminGroup
adminAllowedCreateClasses	<p>List of object classes that can be created by members of an administrative group.</p> <p>Single or multiple value: Multiple, typically chosen from the following list:</p> <p>adminAllocation adminGroup adminPolicy adminRealm adminRole adminTarget domain groupOfNames inetOrgPerson mailDomain mailLocalUserPrefs mailUser mailUserPrefs organization organizationalPerson organizationalUnit person</p> <p>Matching rule: caseIgnoreMatch</p> <p>Syntax type: Directory string</p>	adminRole
adminAllowedDomains	<p>List of domain name patterns that can be used by members of an administrative group creating new e-mail accounts.</p> <p>Patterns have the following form:</p> <p>[*.] [domain-component .] domain-component . top-level-domain</p> <p>Single or multiple value: Multiple</p> <p>Matching rule: caseIgnoreMatch</p> <p>Syntax type: IA5 string</p>	adminGroup

Attribute Name	Definition	Object Classes
adminAllowedUpdateClasses	<p>List of object classes that can be updated by members of an administrative group.</p> <p>Single or multiple value: Multiple, typically chosen from the following list:</p> <ul style="list-style-type: none"> adminAllocation adminGroup adminPolicy adminRealm adminRole adminTarget domain groupOfNames inetOrgPerson mailDomain mailLocalUserPrefs mailUser mailUserPrefs organization organizationalPerson organizationalUnit person <p>Matching rule: caseIgnoreMatch</p> <p>Syntax type: Directory string</p>	adminRole
adminApprovedSendersList	<p>List of SMTP addresses that may send messages to the accounts with mailParentalControl enabled in a realm (which typically represents a family).</p> <p>Single or multiple value: Multiple</p> <p>Matching rule: caseIgnoreMatch</p> <p>Syntax type: Directory string</p>	adminRealm

Attribute Name	Definition	Object Classes
adminAttributeConstraint	<p>Constraint on how an administrator can modify the value of an LDAP attribute. The syntax for specifying a constraint is:</p> <p><version, access-level, attribute-name, constraint [, value...] ></p> <p>Where:</p> <p>version is the syntax version number to accommodate future changes.</p> <p>access-level is the level that an adminRole must have to use this constraint.</p> <p>attribute-name is the name of an attribute.</p> <p>constraint has one of the values listed below.</p> <p>Single or multiple value: Multiple, chosen from the following list:</p> <ul style="list-style-type: none"> • MODIFY, meaning that the value is unconstrained. • NO_MODIFY, meaning that no modification is allowed. This is the default value. • RANGE, meaning that the value must be within a specified range. • MULTIPLE_VALUE_LIMIT, specifying a limit on the number of values an attribute may have. • CHOICE, meaning that the value is one of the specified choices. <p>Matching rule: caseIgnoreMatch</p> <p>Syntax type: Directory string</p> <p>Examples:</p> <p><1, 10, mailQuotaThreshold, RANGE, 10-50></p> <p><1, 50, mailForwarding, NO_MODIFY></p> <p><1, 100, mailForwarding, CHOICE, 0, 1></p>	adminGroup adminPolicy adminRealm

Attribute Name	Definition	Object Classes
adminCreatePeerAdminGroup	<p>Distinguished names of roles for which an administrator can create administrative groups.</p> <p>Single or multiple value: Multiple</p> <p>Matching rule: distinguishedNameMatch</p> <p>Syntax type: Distinguished name, with:</p> <ul style="list-style-type: none"> • DN mapping • Attribute indexing • Enforcement of referential integrity <p>Example: cn=rolePA, cn=admin root</p>	adminRole
adminCreatePeerAdminPolicy	<p>Flag that enables members of this administrative role to create mail policy objects within their own realm.</p> <p>Single or multiple value: Single, one of the following:</p> <p>TRUE FALSE</p> <p>Default value: TRUE</p> <p>Matching rule: booleanMatch</p> <p>Syntax type: Boolean</p>	adminRole
adminCreateRealm	<p>Flag enabling members of this administrative group to create new realms beneath the current realm. The adminTargetDN of the new realm may contain only children of the nodes in the adminTargetDN of the current authority.</p> <p>Single or multiple value: Single, one of the following:</p> <ul style="list-style-type: none"> • TRUE (members of this role can create new authorities) • FALSE (members of this role cannot create new authorities) <p>Default value: TRUE</p> <p>Matching rule: booleanMatch</p> <p>Syntax type: Boolean</p>	adminRole

Attribute Name	Definition	Object Classes
adminCreateSubAdminGroup	<p>Distinguished names of administrative roles for which groups can be created in subordinate realms.</p> <p>Single or multiple value: Multiple</p> <p>Matching rule: distinguishedNameMatch</p> <p>Syntax type: Distinguished name, with:</p> <ul style="list-style-type: none"> • DN mapping • Attribute indexing • Enforcement of referential integrity <p>Example: cn=rolePA, cn=adminRoot</p>	adminRole
adminCreateSubAdminPolicy	<p>Flag that enables members of this role to create mail policy objects in a subordinate authority.</p> <p>Single or multiple value: Single, one of the following:</p> <p>TRUE FALSE</p> <p>Default value: TRUE</p> <p>Matching rule: booleanMatch</p> <p>Syntax type: Boolean</p>	adminRole
adminDefaultCreatedGroups	<p>Administrative groups to be created for a new realm.</p> <p>Matching rule: distinguishedNameMatch</p> <p>Syntax type: Distinguished name, with:</p> <ul style="list-style-type: none"> • DN mapping • Attribute indexing • Enforcement of referential integrity <p>Example:</p> <pre>adminDefaultCreatedGroups: cn=roleSPA,cn=admin root</pre> <p>creates a new administrative group for the site provider administrator role in a new realm.</p>	adminRealmSpec

Attribute Name	Definition	Object Classes
adminDeletePeerAdminGroup	<p>Distinguished names of roles for which administrative groups in the administrator's realm can be deleted by an administrator.</p> <p>Single or multiple value: Multiple</p> <p>Matching rule: distinguishedNameMatch</p> <p>Syntax type: Distinguished name, with:</p> <ul style="list-style-type: none"> • DN mapping • Attribute indexing • Enforcement of referential integrity <p>Example: cn=rolePA, cn=admin root</p>	adminRole
adminDeletePeerAdminPolicy	<p>Flag that enables members of this administrative role to delete mail policy entries within their own realm.</p> <p>Single or multiple value: Single, one of the following:</p> <p>Values: TRUE FALSE</p> <p>Default value: TRUE</p> <p>Matching rule: booleanMatch</p> <p>Syntax type: Boolean</p>	adminRole
adminDeleteRealm	<p>Flag that enables members of this administrative group to delete realms. They may delete only realms beneath the current realm that have no child entries remaining.</p> <p>Single or multiple value: Single, one of the following:</p> <ul style="list-style-type: none"> • TRUE (members may delete realms) • FALSE (members may not delete realms) <p>Default value: TRUE</p> <p>Matching rule: booleanMatch</p> <p>Syntax type: Boolean</p>	adminRole

Attribute Name	Definition	Object Classes
adminDeleteSubAdminGroup	<p>Distinguished names of roles for which administrative groups may be deleted in subordinated realms.</p> <p>Single or multiple value: Multiple</p> <p>Matching rule: distinguishedNameMatch</p> <p>Syntax type: Distinguished name, with:</p> <ul style="list-style-type: none"> • DN mapping • Attribute indexing • Enforcement of referential integrity 	adminRole
adminDeleteSubAdminPolicy	<p>Flag that enables members of this role to delete mail policy objects in a subordinate authority.</p> <p>Single or multiple value: Single, one of the following:</p> <p>TRUE FALSE</p> <p>Default value: TRUE</p> <p>Matching rule: booleanMatch</p> <p>Syntax type: Boolean</p>	adminRole
adminDomainSpecControl	<p>Single or multiple value: Single</p> <p>Matching rule: booleanMatch</p> <p>Syntax type: Boolean</p>	adminRealmSpec
adminLastLogin	<p>Time stamp of this administrative user's last login to the InterManager GUI.</p> <p>Single or multiple value: Single</p> <p>Matching rule: caseIgnoreMatch</p> <p>Syntax type: Directory string</p>	adminUserPrefs
adminMaxDomains	<p>Maximum number of domains that may be created.</p> <p>Single or multiple value: Single</p> <p>Matching rule: integerMatch</p> <p>Syntax type: Integer</p>	adminAllocation
adminMaxIMAP	<p>Maximum number of IMAP4 user licenses.</p> <p>Single or multiple value: Single</p> <p>Matching rule: integerMatch</p> <p>Syntax type: Integer</p>	adminAllocation

Attribute Name	Definition	Object Classes
adminMaxIMAPSSL	Maximum number of IMAP4 users with SSL enabled. Single or multiple value: Single Matching rule: integerMatch Syntax type: Integer	adminAllocation
adminMaxInterManager	Maximum number of accounts that have InterManager enabled. Single or multiple value: Single Matching rule: integerMatch Syntax type: Integer	adminAllocation
adminMaxMailingLists	Maximum number of mailing lists that can be created from an adminAllocation object. Single or multiple value: Single Matching rule: integerMatch Syntax type: Integer	adminAllocation
adminMaxPOP	Maximum number of POP3 users licensed. Single or multiple value: Single Matching rule: integerMatch Syntax type: Integer	adminAllocation
adminMaxPOPSSL	Maximum number of POP3 users with SSL enabled. Single or multiple value: Single Matching rule: integerMatch Syntax type: Integer	adminAllocation
adminMaxRealms	Maximum number of adminRealms. Single or multiple value: Single Matching rule: integerMatch Syntax type: Integer	adminAllocation
adminMaxSelfCare	Maximum number of accounts that have SelfCare enabled. Single or multiple value: Single Matching rule: integerMatch Syntax type: Integer	adminAllocation

Attribute Name	Definition	Object Classes
adminMaxSmtpt	<p>Maximum number of accounts that are permitted to send mail using SMTP protocol.</p> <p>Single or multiple value: Single</p> <p>Matching rule: integerMatch</p> <p>Syntax type: Integer</p>	adminAllocation
adminMaxSMTPSSL	<p>Maximum number of SMTP licenses with SSL enabled.</p> <p>Single or multiple value: Single</p> <p>Matching rule: integerMatch</p> <p>Syntax type: Integer</p>	adminAllocation
adminMaxStorageKB	<p>Maximum storage space, in kilobytes, that can be allocated to all accounts combined.</p> <p>Single or multiple value: Single</p> <p>Matching rule: integerMatch</p> <p>Syntax type: Integer</p>	adminAllocation
adminMaxUsers	<p>Maximum number of licensed users.</p> <p>Single or multiple value: Single</p> <p>Matching rule: integerMatch</p> <p>Syntax type: Integer</p> <p>Default value: 1000</p>	adminAllocation
adminMaxWebMail	<p>Maximum number of accounts that have WebEdge enabled.</p> <p>Single or multiple value: Single</p> <p>Matching rule: integerMatch</p> <p>Syntax type: Integer</p>	adminAllocation
adminMinAllowedAccessLevel	<p>Minimum access level an administrator may have in order to create a specified realm.</p> <p>Single or multiple value: Single</p> <p>Matching rule: integerMatch</p> <p>Syntax type: Integer</p>	adminRealmSpec
adminNumDomains	<p>Current number of realms created or allocated.</p> <p>Single or multiple value: Single</p> <p>Matching rule: integerMatch</p> <p>Syntax type: Integer</p>	adminAllocation

Attribute Name	Definition	Object Classes
adminNumIMAP	Current number of IMAP4 users. Single or multiple value: Single Matching rule: integerMatch Syntax type: Integer	adminAllocation
adminNumIMAPSSL	Current number of IMAP4 users with SSL enabled. Single or multiple value: Single Matching rule: integerMatch Syntax type: Integer	adminAllocation
adminNumInterManager	Current number of accounts with InterManager enabled. Single or multiple value: Single Matching rule: integerMatch Syntax type: Integer	adminAllocation
adminNumMailingLists	Number of mailing lists currently allocated from any adminAllocation object. Single or multiple value: Single Matching rule: integerMatch Syntax type: Integer	adminAllocation
adminNumPOP	Current number of POP3 users. Single or multiple value: Single Matching rule: integerMatch Syntax type: Integer	adminAllocation
adminNumPOPSSL	Current number of POP3 users with SSL enabled. Single or multiple value: Single Matching rule: integerMatch Syntax type: Integer	adminAllocation
adminNumRealms	Current number of realms created or allocated. Single or multiple value: Single Matching rule: integerMatch Syntax type: Integer	adminAllocation

Attribute Name	Definition	Object Classes
adminNumSelfCare	<p>Current number of accounts that have SelfCare enabled.</p> <p>Single or multiple value: Single</p> <p>Matching rule: integerMatch</p> <p>Syntax type: Integer</p>	adminAllocation
adminNumSmtP	<p>Current number of accounts that have SMTP access enabled.</p> <p>Single or multiple value: Single</p> <p>Matching rule: integerMatch</p> <p>Syntax type: Integer</p>	adminAllocation
adminNumSMTPSSL	<p>Current number of SMTP licenses with SSL enabled.</p> <p>Single or multiple value: Single</p> <p>Matching rule: integerMatch</p> <p>Syntax type: Integer</p>	adminAllocation
adminNumUsers	<p>Current number of accounts created or allocated within this realm.</p> <p>Single or multiple value: Single</p> <p>Matching rule: integerMatch</p> <p>Syntax type: Integer</p>	adminAllocation
adminNumWebMail	<p>Current number of accounts created or allocated that have WebEdge enabled.</p> <p>Single or multiple value: Single</p> <p>Matching rule: integerMatch</p> <p>Syntax type: Integer</p>	adminAllocation
adminParentAdminPolicy	<p>Distinguished name of the parent adminPolicy entry. This adminPolicy must have a smaller or equal number of permissions than the parent policy.</p> <p>Single or multiple value: Single</p> <p>Matching rule: distinguishedNameMatch</p> <p>Syntax type: Distinguished name, with:</p> <ul style="list-style-type: none"> • DN mapping • Attribute indexing • Enforcement of referential integrity 	adminPolicy

Attribute Name	Definition	Object Classes
adminParentalRejectAction	<p>Flag to control the handling of messages that are blocked by parental control. This is typically used by family mailbox groups only.</p> <p>Single or multiple value: Single, one of the following:</p> <ul style="list-style-type: none"> • D (drop) causes the messages to be discarded. This is the default value. • F (forward) causes the messages to be forwarded to the head of the household. <p>Matching rule: caseIgnoreMatch</p> <p>Syntax type: Directory string</p>	adminRealm
adminParentDomains	<p>List of fully-qualified domain names. New mailDomain objects must have domains subordinate to a parent domain.</p> <p>Single or multiple value: Multiple</p> <p>Matching rule: caseIgnoreMatch</p> <p>Syntax type: IA5 string</p>	adminGroup
adminPolicyDefaultDN	<p>Mail policy used for any account in which the adminPolicy object class is not specified.</p> <p>Single or multiple value: Single</p> <p>Matching rule: distinguishedNameMatch</p> <p>Syntax type: Distinguished name, with:</p> <ul style="list-style-type: none"> • DN mapping • Attribute indexing • Enforcement of referential integrity 	adminRoot
adminPolicyDN	<p>Distinguished name of the mail policy object for a mailUser object.</p> <p>Single or multiple value: Single</p> <p>Constraint: The LDAP object pointed to by this attribute must exist in the directory.</p> <p>Matching rule: distinguishedNameMatch</p> <p>Syntax type: Distinguished name, with:</p> <ul style="list-style-type: none"> • DN mapping • Attribute indexing • Enforcement of referential integrity <p>Example: adminPolicyDN: cn=full, cn=admin root</p>	mailUser

Attribute Name	Definition	Object Classes
adminPolicyDNUsed	<p>Single or multiple value: Multiple</p> <p>Matching rule: distinguishedNameMatch</p> <p>Syntax type: Distinguished name, with:</p> <ul style="list-style-type: none"> • DN mapping • Attribute indexing • Enforcement of referential integrity 	adminAllocation
adminPolicyGrantDN	<p>List of distinguished names of adminPolicy objects. Used as templates to create new adminPolicy objects for the adminRealm.</p> <p>Single or multiple value: Multiple</p> <p>Matching rule: distinguishedNameMatch</p> <p>Syntax type: Distinguished name, with:</p> <ul style="list-style-type: none"> • DN mapping • Attribute indexing • Enforcement of referential integrity <p>Default value: cn=full, cn=adminRoot</p>	adminRealm
adminPreferredLocale	<p>Internationalization locale, meaning the language and time and date representation preferred by this administrative user. This is used in the InterManager GUI.</p> <p>Single or multiple value: Single</p> <p>Matching rule: caseIgnoreMatch</p> <p>Syntax type: Directory string</p>	adminUserPrefs
adminProvisionOnly	<p>Flag which, if set to TRUE, constrains the adminPolicy so that it can be used only to provision accounts. If set to FALSE, it can be used as a template for a derived adminPolicy object.</p> <p>Single or multiple value: Single, one of the following:</p> <p>TRUE FALSE</p> <p>Matching rule: booleanMatch</p> <p>Syntax type: Boolean</p>	adminPolicy

Attribute Name	Definition	Object Classes
adminRealmDN	<p>Distinguished name of the realm with administrative control over an application entry.</p> <p>Single or multiple value: Single</p> <p>Default value: cn=site, cn=admin root</p> <p>Constraint: Must refer to an existing adminRealm object.</p> <p>Matching rule: distinguishedNameMatch</p> <p>Syntax type: Distinguished name, with:</p> <ul style="list-style-type: none"> • DN mapping • Attribute indexing • Enforcement of referential integrity 	adminTarget
adminRealmType	<p>Type of realm.</p> <p>Single or multiple value: Single, one of the following:</p> <p>provider org ou family</p> <p>Matching rule: caseIgnoreMatch</p> <p>Syntax type: Printable string</p>	adminRealmSpec
adminRoleDN	<p>Distinguished name of the adminRole for the adminGroup. Describes the generic privileges for the group.</p> <p>Single or multiple value: Single</p> <p>Matching rule: distinguishedNameMatch</p> <p>Syntax type: Distinguished name, with:</p> <ul style="list-style-type: none"> • DN mapping • Attribute indexing • Enforcement of referential integrity 	adminGroup
adminSuperiorAttributeConstraint	<p>Set of attribute constraints on updates to this administrative group or realm by administrators in a group having superior authority.</p> <p>Single or multiple value: Multiple</p> <p>Matching rule: caseIgnoreMatch</p> <p>Syntax type: Directory string</p>	adminGroup adminRealm

Attribute Name	Definition	Object Classes
adminTargetDN	<p>List of distinguished names of the top of one or more directory subtrees over which an adminRealm object has control.</p> <p>Single or multiple value: Multiple</p> <p>Matching rule: distinguishedNameMatch</p> <p>Syntax type: Distinguished name, with:</p> <ul style="list-style-type: none"> • DN mapping • Attribute indexing • Enforcement of referential integrity 	adminRealm
adminTargetObjectClass	<p>Type of application tree entry to create when creating a new realm.</p> <p>Single or multiple value: Multiple, from the following:</p> <p>provider org ou family</p> <p>Matching rule: caseIgnoreMatch</p> <p>Syntax type: Printable string</p>	adminRealmSpec
adminTemplateOnly	<p>Flag which, if set to TRUE, constrains the adminPolicy so that it can be used only as the template for derived adminPolicy objects. If set to FALSE, it can be used to provision an account.</p> <p>Single or multiple value: Single, one of the following:</p> <p>TRUE FALSE</p> <p>Matching rule: booleanMatch</p> <p>Syntax type: Boolean</p>	adminPolicy

Attribute Name	Definition	Object Classes
adminUsedStorageKB	<p>Storage space, in kilobytes, currently allocated to accounts. This is the sum of the mailQuotaTotKB attributes for all accounts in the adminRealm that maintains allocation data. If there are subordinate realms that maintain allocation data, the sum includes the mailQuotaMaxKB value for those subordinate realms (but not for any subordinates of subordinates).</p> <p>Single or multiple value: Single Matching rule: integerMatch Syntax type: Integer</p>	adminAllocation
aliasedObjectName	<p>Used if the entry containing this attribute is an alias.</p> <p>Single or multiple value: Single Matching rule: distinguishedNameMatch Syntax type: Distinguished name RFC: 2256 paragraph 5.2</p>	alias
attributeTypes	<p>Single or multiple value: Multiple Matching rule: objectIdentifierFirstComponentMatch Syntax type: Attribute type description RFC: 2252 paragraphs 5.1.6 and 6.1</p>	subschema
audio	<p>Allows the storage of sounds in the directory.</p> <p>Single or multiple value: Multiple Constraint: Maximum number of characters in string is 250,000. Matching rule: octetStringMatch Syntax type: Octet string RFC: 1274 paragraph 9.3.45</p>	inetOrgPerson
authorityRevocationList	<p>To be stored and requested in binary form, as authorityRevocationList;binary.</p> <p>Single or multiple value: Multiple Syntax type: Certificate list RFC: 2256 paragraph 5.39</p>	certificationAuthority cRLDistributionPoint

Attribute Name	Definition	Object Classes
billingID	Customer-specified identifier for billing purposes. Single or multiple value: Single Matching rule: caseExactMatch Syntax type: Directory string	adminRealm mailUser
businessCategory	Type of business performed by an organization. Single or multiple value: Multiple Constraint: Maximum length of the string is 128 characters. Matching rule: caseIgnoreMatch Syntax type: Directory string RFC: 2256 paragraph 5.16	dmd domain groupOfNames groupOfUniqueNames inetOrgPerson organization organizationalUnit residentialPerson
c	Two-letter ISO 3166 country code. Single or multiple value: Single Matching rule: caseIgnoreMatch Syntax type: Directory string RFC: 2256 paragraph 5.7	country
cACertificate	Attribute to be stored and requested in binary form, as <code>cACertificate;binary</code> . Single or multiple value: Multiple Syntax type: Certificate RFC: 2256 paragraph 5.38	certificationAuthority
carLicense	Vehicle license plate or registration. Single or multiple value: Multiple Matching rule: caseIgnoreMatch Syntax type: Directory string RFC: Draft-smith-ldap-inetorgperson-03; paragraph 5.1	inetOrgPerson
certificateRevocationList	Attribute to be stored and requested in binary form, as <code>certificateRevocationList;binary</code> . Single or multiple value: Multiple Syntax type: Certificate list RFC: 2256 paragraph 5.40	certificationAuthority cRLDistributionPoint

Attribute Name	Definition	Object Classes
changeLog	Distinguished name of the entry that contains the set of server changelog entries. Single or multiple value: Multiple Matching rule: distinguishedNameMatch Syntax type: Distinguished name	dseRoot
changeNumber	Number that uniquely identifies a change made to a directory entry. Single or multiple value: Single Matching rule: caseIgnoreMatch Syntax type: Printable string	changeLogEntry
changes	Set of changes to be applied to an entry. Single or multiple value: Multiple Matching rule: none Syntax type: Octet string	changeLogEntry
changeType	Type of change to be made to an entry. Single or multiple value: Multiple Matching rule: caseIgnoreMatch Syntax type: Directory string	changeLogEntry

Attribute Name	Definition	Object Classes
cn	<p>Common name, representing the name of an object.</p> <ul style="list-style-type: none"> In <code>adminPolicy</code>, cn is the name of the policy. In <code>adminRealm</code>, it is the name of the realm. In <code>adminRole</code>, it is the name of the role. <p>Default value: <code>roleSPA</code></p> <ul style="list-style-type: none"> In <code>adminRoot</code>, it is the name of the entry at the root of the DIT. In <code>groupOfNames</code>, it is the name of the group. In <code>partition</code>, it is the name of the partition. In <code>person</code>, it is the full name of the person. In <code>replAgreement</code>, it is the name of the replication agreement. <p>Single or multiple value: Multiple Matching rule: <code>caseIgnoreMatch</code> Syntax type: Directory string RFC: 2256 paragraph 5.4</p>	<p>adminAllocCounts adminPolicy adminRealm adminRole adminRoot applicationEntity applicationProcess cRLDistributionPoint device groupOfNames groupOfUniqueNames organizationalRole partition person replAgreement scConfig scConfigRoot</p>
consumerIdentity	<p>Distinguished name the consumer (Directory Cache server) uses to bind to the supplier (Directory server) to read changelog entries.</p> <p>The default value is the value of <code>ldapRootDN</code> configuration variable of the Directory server.</p> <p>Single or multiple value: Single Default value: The value of the <code>ldapRootPwD</code> configuration variable of the Directory server Matching rule: <code>distinguishedNameMatch</code> Syntax type: Distinguished name</p>	<p>replAgreement</p>

Attribute Name	Definition	Object Classes
consumerPassword	<p>LDAP password used by the consumer (Directory Cache server) to bind to the supplier (Directory server).</p> <p>Single or multiple value: Single</p> <p>Constraint: Maximum length is 128 characters.</p> <p>Matching rule: octetStringMatch</p> <p>Syntax type: Octet string</p>	replAgreement
contactInfo	<p>Contact information in free-form text. Typically contains white pages information such as telephone numbers.</p> <p>Single or multiple value: Multiple</p> <p>Matching rule: caseIgnoreMatch</p> <p>Syntax type: Printable string</p>	adminGroup adminRealm
createTimeStamp	<p>Attribute that should appear with each entry, representing the date and time when the entry was created.</p> <p>Single or multiple value: Single</p> <p>Matching rule: generalizedTimeMatch</p> <p>Ordering: generalized Time OrderingMatch</p> <p>Syntax type: Generalized time</p> <p>RFC: 2252 paragraph 5.1.1</p>	N/A (Directory operational attribute)
creatorsName	<p>Attribute that should appear with each entry, representing the distinguished name of the user who created it.</p> <p>Single or multiple value: Single</p> <p>Matching rule: distinguishedNameMatch</p> <p>Syntax type: Distinguished name, with:</p> <ul style="list-style-type: none"> • DN mapping <p>RFC: 2252 paragraph 5.1.3</p>	N/A (Directory operational attribute)
crossCertificatePair	<p>Attribute to be stored and requested in binary form, as <code>crossCertificatePair;binary</code>.</p> <p>Single or multiple value: Multiple</p> <p>Syntax type: Certificate pair</p> <p>RFC: 2256 paragraph 5.41</p>	certificateAuthority

Attribute Name	Definition	Object Classes
dc	<p>Domain component. The value of the dc attribute is a string holding one component of a domain name.</p> <p>Single or multiple value: Single</p> <p>Matching rule: caeIgnoreIA5Match</p> <p>Substrings matching rule: caseIgnoreIA5SubstringsMatch</p> <p>Syntax type: IA5 string</p>	dcObject domain
deleteOldRDN	<p>Flag indicating whether the old relative distinguished name (RDN) should be retained as an attribute of the entry whose RDN was modified.</p> <p>Single or multiple value: Single, one of the following:</p> <p>TRUE</p> <p>FALSE</p> <p>Matching rule: booleanMatch</p> <p>Syntax type: Boolean</p>	changeLogEntry
deltaRevocationList	<p>This attribute is to be stored and requested in binary form, as <code>deltaRevocationList.binary</code>.</p> <p>Single or multiple value: Multiple</p> <p>Syntax type: Certificate list</p> <p>RFC: 2256 paragraph 5.54</p>	certificationAuthority-V2 cRLDistributionPoint
departmentNumber	<p>Department within an organization.</p> <p>Single or multiple value: Multiple</p> <p>Matching rule: caseIgnoreMatch</p> <p>Syntax type: Directory string</p> <p>RFC: Draft-smith-ldap-inetorgperson-03; paragraph 5.2</p>	inetOrgPerson

Attribute Name	Definition	Object Classes
description	<p>Description of an object; the description is readable by humans.</p> <p>Single or multiple value: Multiple</p> <p>Constraint: Maximum length of string is 1024 characters.</p> <p>Matching rule: caseIgnoreMatch</p> <p>Syntax type: Directory string</p> <p>RFC: 2256 paragraph 5.14</p>	<p>adminPolicy applicationEntity applicationProcess country device dmd domain groupOfNames groupOfUniqueNames locality organization organizationalRole organizationalUnit person</p>
destinationIndicator	<p>Destination used for telegram service.</p> <p>Single or multiple value: Multiple</p> <p>Constraint: Maximum length of the string is 128 characters.</p> <p>Matching rule: caseIgnoreMatch</p> <p>Syntax type: Printable string</p> <p>RFC: 2256 paragraph 5.28</p>	<p>dmd domain organization organizationalPerson organizationalRole organizationalUnit residentialPerson</p>
displayName	<p>Preferred name of a person to be used when displaying entries.</p> <p>Single or multiple value: Single</p> <p>Matching rule: caseIgnoreMatch</p> <p>Syntax type: Directory string</p> <p>RFC: Draft-smith-ldap-inetorgperson-03; paragraph 5.3</p>	<p>inetOrgPerson</p>
distinguishedName	<p>Base attribute from which the attributes with Distinguished name syntax inherit.</p> <p>Single or multiple value: Multiple</p> <p>Matching rule: distinguishedNameMatch</p> <p>Syntax type: Distinguished name</p> <p>RFC: 2256 paragraph 5.50</p>	<p>N/A</p>
ditContentRules	<p>Single or multiple value: Multiple</p> <p>Matching rule: objectIdentifierFirstComponentMatch</p> <p>Syntax type: DIT content rule description</p> <p>RFC: 2252 paragraphs 5.4.3 and 6.11</p>	<p>subschema</p>

Attribute Name	Definition	Object Classes
ditStructureRules	<p>Single or multiple value: Multiple</p> <p>Matching rule: integerFirstComponentMatch</p> <p>Syntax type: DIT structure rule description</p> <p>RFC: 2252 paragraphs 5.4.1 and 6.33</p>	subschema
dmdName	<p>Specification of a directory management domain (DMD), which is the administrative authority that operates the Directory server.</p> <p>Single or multiple value: Multiple</p> <p>Matching rule: caseIgnoreMatch</p> <p>Syntax type: Directory string</p> <p>RFC: 2256 paragraph 5.55</p>	dmd
domainName	<p>Complete domain associated with a mailDomain object.</p> <p>Single or multiple value: Single</p> <p>Constraints:</p> <ul style="list-style-type: none"> • Must be unique. • Maximum length is 255 characters. <p>Matching rule: caseIgnoreMatch</p> <p>Syntax type: IA5 string</p> <p>Example: software.com</p>	mailDomain

Attribute Name	Definition	Object Classes
domainType	<p>Domain type. There are three types of domains:</p> <ul style="list-style-type: none"> • Local domain – an authoritative domain for which InterMail claims exclusive control. The InterMail system is the ultimate destination for mail addressed to a local domain. Mail addressed to non-existent recipients within a local domain is considered undeliverable, and is returned to the sender. • Non-authoritative (semi-local) domain – allows the mail system to accept mail for the domain and relay it to another mail host if the recipient is not recognized. The other mail host is specified in the <code>mailRelayHost</code> attribute. <p>This domain type is used, for example, during migration of e-mail accounts from a legacy mail system to InterMail, or to define domains for which your site is used as a backup.</p> <ul style="list-style-type: none"> • Rewrite domain – defines a rule for rewriting the recipient address of incoming mail. It must be associated with a local or non-authoritative domain. <p>If the domain of the recipient address is defined as a rewrite domain, the address is rewritten to include the address of the associated local or non-authoritative domain.</p> <p>This domain type allows accounts to receive messages addressed to the same user in multiple domains without requiring SMTP aliases for each account.</p> <p>Single or multiple value: Single, one of the following:</p> <ul style="list-style-type: none"> • L (for local domains) • N (for non-authoritative domains) • R (for rewrite domains) <p>Matching rule: <code>caseExactMatch</code></p> <p>Syntax type: Printable string</p>	mailDomain

Attribute Name	Definition	Object Classes
employeeNumber	Numerical identification of an employee within an organization. Single or multiple value: Single Matching rule: caseIgnoreMatch Syntax type: Directory string RFC: Draft-smith-ldap-inetorgperson-03; paragraph 5.4	inetOrgPerson
employeeType	Identifies type of employment for a person. Single or multiple value: Multiple; any value may be used, such as: Contractor Employee Intern Temp External Unknown Matching rule: caseIgnoreMatch Syntax type: Directory string RFC: Draft-smith-ldap-inetorgperson-03.txt; paragraph 5.5	inetOrgPerson
enhancedSearchGuide	Attribute used by X.500 clients to construct search filters. Single or multiple value: Multiple Matching rule: none Syntax type: Enhanced Guide RFC: 2256 paragraph 5.48	dmd domain locality organization organizationalUnit
facsimileTelephoneNumber	Fax telephone number. Single or multiple value: Multiple Matching rule: none Syntax type: Facsimile telephone number RFC: 2256 paragraph 5.24	country dmd domain organization organizationalPerson organizationalRole organizationalUnit residentialPerson
givenName	First name of a person. Single or multiple value: Multiple Matching rule: caseIgnoreMatch Syntax type: Directory string RFC: 2256 paragraph 5.43	inetOrgPerson

Attribute Name	Definition	Object Classes
homePhone	<p>Home telephone number for a person.</p> <p>Single or multiple value: Multiple, with each following the format for international telephone numbers</p> <p>Matching rule: telephoneNumberMatch</p> <p>Syntax type: Telephone number</p> <p>Example: +44 71 123 4567</p> <p>RFC: 1274 paragraph 9.3.16</p>	inetOrgPerson
homePostalAddress	<p>Home address for a person.</p> <p>Single or multiple value: Multiple</p> <p>Constraint: Limited to up to 6 lines of 30 characters each.</p> <p>Matching rule: caseIgnoreListMatch</p> <p>Syntax type: Postal address</p> <p>RFC: 1274 paragraph 9.2.29</p>	inetOrgPerson
initials	<p>Initials of a person's given name and/or middle name.</p> <p>Single or multiple value: Multiple</p> <p>Matching rule: caseIgnoreMatch</p> <p>Syntax type: Directory string</p> <p>RFC: 2256 paragraph 5.44</p>	inetOrgPerson
internationalISDNNumber	<p>Single or multiple value: Multiple</p> <p>Constraint: Maximum length of the string is 16 characters.</p> <p>Matching rule: numericStringMatch</p> <p>Syntax type: Numeric string</p> <p>RFC: 2256 paragraph 5.26</p>	dmd domain organization organizationalPerson organizationalRole organizationalUnit residentialPerson
jpegPhoto	<p>One or more JPEG images of a person using the JPEG file interchange format.</p> <p>Single or multiple value: Multiple</p> <p>Matching rule: none</p> <p>Syntax type: JPEG</p> <p>RFC: Draft-smith-ldap-inetorgperson-03; paragraph 5.6</p>	inetOrgPerson

Attribute Name	Definition	Object Classes
1	<p>Name of a locality, such as a city, county, or other geographic region.</p> <p>Single or multiple value: Multiple</p> <p>Matching rule: caseIgnoreMatch</p> <p>Syntax type: Directory string</p> <p>RFC: 2256 paragraph 5.8</p>	applicationEntity applicationProcess device dmd domain locality organization organizationalPerson organizationalRole organizationalUnit residentialPerson
labeledURI	<p>Storage location for Uniform Resource Locators (URL) and other types of Uniform Resource Identifiers (URI) in a directory entry. The syntax is:</p> <p><URI>/<label></p> <p>Where <code>label</code> describes the resource to which the URI points.</p> <p>Single or multiple value: Multiple</p> <p>Matching rule: caseExactMatch</p> <p>Syntax type: Directory string</p> <p>Example: <code>http://www.software.com/Software.com home page</code></p> <p>RFC: 2079</p>	adminUserPrefs inetOrgPerson
lastChangeNumber	<p>Number of the last change written to the change log.</p> <p>Single or multiple value: Single</p> <p>Matching rule: caseIgnoreMatch</p> <p>Syntax type: Printable string</p>	replAgreement
mail	<p>Primary SMTP e-mail address for a person. The value of this attribute uniquely identifies a user.</p> <p>Single or multiple value: Single</p> <p>Constraint: The maximum number of characters in the string is 256.</p> <p>Matching rule: caseIgnoreIA5Match</p> <p>Syntax type: IA5 string</p> <p>Example: <code>mail: john.doe@software.com</code></p> <p>RFC: 822</p>	inetOrgPerson mailUser

Attribute Name	Definition	Object Classes
mailAllowTheseIps	<p>Specification of a set of IP addresses from which a user is allowed to access the POP and IMAP servers (and the SMTP server if SMTP authentication is required).</p> <p>The list of IP addresses is of the form: D.D.D.D[/N]</p> <p>Where:</p> <ul style="list-style-type: none"> • D is a number from 0 to 255. • N is a number from 0 to 32. <p>Single or multiple value: Multiple</p> <p>Constraint: Maximum length is 64 characters.</p> <p>Matching rule: caseIgnoreMatch</p> <p>Syntax type: Printable string</p>	mailUserPrefs
mailAlternateAddress	<p>Alternate e-mail addresses for the recipient.</p> <p>Single or multiple value: Multiple</p> <p>Constraints:</p> <ul style="list-style-type: none"> • Each value of this attribute must uniquely identify a user. • The domain part of an address must exist as a domainName attribute of a mailDomain object. It must be local or non-authoritative. • The maximum number of characters in the string is 256. <p>Matching rule: caseIgnoreIA5Match</p> <p>Syntax type: IA5 string</p> <p>Example: nickname@software.com</p> <p>RFC: Section 3.2 of Internet Draft http://search.ietf.org/internet-draft-lachman-ldap-mail-routing-03.txt.</p>	mailUser
mailAutoReplyHost	<p>MSS host that stores the user's auto-reply message.</p> <p>Single or multiple value: Single, which can be any valid host name</p> <p>Constraint: Maximum length is 255 characters.</p> <p>Matching rule: caseIgnoreIA5Match</p> <p>Syntax type: IA5 string</p>	mailUser

Attribute Name	Definition	Object Classes
mailAutoReplyMode	<p>Attribute that returns the account's auto-reply message to the sender, unless the value is set to <code>None</code>.</p> <p>Single or multiple value: Single, one of the following:</p> <ul style="list-style-type: none"> • <code>N</code> (none) means that the message is not returned. • <code>R</code> (reply mode) sends the auto-reply message every time mail is sent to the account. Used to automatically distribute sales information, directions, and so on. • <code>E</code> (echo mode) is the same as <code>Reply</code>, but also includes the sender's original message as a MIME attachment to the auto-reply message. • <code>V</code> (vacation mode) sends only one copy of the auto-reply message to each sender during the defined vacation period, even if that sender sends multiple messages to the account. <p>Default value: <code>N</code></p> <p>Matching rule: <code>caseIgnoreMatch</code></p> <p>Syntax type: Printable string</p> <p>RFC: Section 10 of Internet Draft http://search.ietf.org/internet-draft-lachman-ldap-mail-routing-03.txt.</p>	mailUserPrefs
mailboxId	<p>Internal identifier for the account's mailbox. Uniquely identifies the user.</p> <p>Single or multiple value: Single</p> <p>Constraint: Maximum length is 38 characters.</p> <p>Matching rule: <code>caseExactMatch</code></p> <p>Syntax type: Numeric string</p>	mailUser

Attribute Name	Definition	Object Classes
mailboxStatus	<p>Status of the user's mailbox.</p> <p>Single or multiple value: Single, one of the following:</p> <ul style="list-style-type: none"> • A (active) status is the most common account status; messages are sent and received normally. • M (maintenance) status means that the mailbox is temporarily unavailable. For example, if the database is shut down for reorganization, the mailboxes in that database cannot accept new messages and cannot answer client requests for mail. Arriving messages are queued for delivery when the status of the account is reset to active. • S (suspended) status prevents access to the account's mailbox, usually because bills have not been paid. Incoming mail is returned to sender. • L (locked) status is identical to S (suspended) status. • D (deleted) status halts mail activity for the account. Mail is treated as undeliverable. Client requests to access the mailbox through the POP or IMAP server are rejected with an unknown username/password error. The account may be restored by resetting its status. • P (proxy) status is used when migrating accounts to a new mail system. Incoming mail is redirected to the proxy MTA (<code>mailSMTPRelayHost</code>) defined for the account. Client requests to retrieve messages through the POP or IMAP server are redirected to the account's proxy POP or IMAP server (<code>mailPOPProxyHost</code>). <p>Constraints: The string can have only one character.</p> <p>Default value: A</p> <p>Matching rule: caseExactMatch</p> <p>Syntax type: Printable string</p>	mailUser

Attribute Name	Definition	Object Classes
mailBypassAuthentication	<p>Flag to allow login using a stored password for SelfCare and WebEdge.</p> <p>Single or multiple value: Single</p> <p>Default value: 0</p> <p>Matching rule: integerMatch</p> <p>Syntax type: Integer</p>	mailUserPrefs
mailDeliveryOption	<p>Flag to set the delivery option. When forwarding is enabled, local delivery can be enabled or disabled. When forwarding is disabled, N is not a valid value.</p> <p>Single or multiple value: Single, one of the following:</p> <ul style="list-style-type: none"> • N (meaning localDeliveryOff) • P (meaning localDeliveryOn) • S (meaning listServer) • E (meaning listExploder) <p>Default value: P</p> <p>Constraints: Accounts that use P are subject to mailbox quotas.</p> <p>Matching rule: caseIgnoreMatch</p> <p>Syntax type: Printable string</p> <p>RFC: Section 10 of Internet Draft http://search.ietf.org/internet-draft-lachman-ldap-mail-routing-03.txt.</p>	mailUserPrefs
mailForwarding	<p>Flag to enable/disable mail forwarding by the MTA to the addresses listed in mailForwardingAddress.</p> <p>Single or multiple value: Single, one of the following:</p> <ul style="list-style-type: none"> • 1 (enabled) • 0 (disabled) <p>Default value: 0</p> <p>Matching rule: integerMatch</p> <p>Syntax type: Integer</p>	mailUserPrefs

Attribute Name	Definition	Object Classes
mailForwardingAddress	<p>Specification of the SMTP addresses to which mail is to be forwarded.</p> <p>Single or multiple value: Multiple</p> <p>Constraint: Maximum length is 256 characters.</p> <p>Matching rule: none</p> <p>Syntax type: IA5 string</p> <p>RFC: Section 10 of Internet Draft http://search.ietf.org/internet-draft-lachman-ldap-mail-routing-03.txt.</p>	mailUser
mailIMAPAccess	<p>Flag to control account access to standard (unencrypted) IMAP service.</p> <p>Single or multiple value: Single, one of the following:</p> <p>all trusted none</p> <p>Default value: all</p> <p>Matching rule: caseIgnoreMatch</p> <p>Syntax type: Printable string</p>	mailUserPrefs
mailIMAPSSLAccess	<p>Flag to control account access to the SSL encrypted IMAP service.</p> <p>Single or multiple value: Single, one of the following:</p> <p>all trusted none</p> <p>Default value: all</p> <p>Matching rule: caseIgnoreMatch</p> <p>Syntax type: Printable string</p>	mailUserPrefs
mailInterManager	<p>Flag to enable account access to the InterManager Web interface.</p> <p>Single or multiple value: Single, one of the following:</p> <ul style="list-style-type: none"> • 1 (enable) • 0 (not enabled) <p>Default value: 1</p> <p>Matching rule: integerMatch</p> <p>Syntax type: Integer</p>	mailUserPrefs

Attribute Name	Definition	Object Classes
mailInterManagerSSL	<p>Flag to enable account access to the SSL-encrypted InterManager Web interface.</p> <p>Single or multiple value: Single, one of the following:</p> <ul style="list-style-type: none"> • 1 (enable) • 0 (not enabled) <p>Default value: 1</p> <p>Matching rule: integerMatch</p> <p>Syntax type: Integer</p>	mailUserPrefs
mailLdapAccess	<p>Flag to control account access to standard LDAP service.</p> <p>Single or multiple value: Single, one of the following:</p> <p>all trusted none</p> <p>Default value: all</p> <p>Matching rule: caseIgnoreMatch</p> <p>Syntax type: Printable string</p>	mailUserPrefs
mailLogin	<p>Login name. This could be the POP name, the IMAP name, or the Mail User Agent name. This name uniquely identifies the user.</p> <p>Single or multiple value: Single</p> <p>Constraint: Maximum length is 129 characters.</p> <p>Matching rule: caseIgnoreMatch</p> <p>Syntax type: Directory string</p>	mailUser

Attribute Name	Definition	Object Classes
mailMessageStore	<p>Name of the host to which a user's messages are delivered, and from which mail is retrieved by the POP and IMAP servers.</p> <p>Single or multiple value: Single</p> <p>Matching rule: caseIgnoreMatch</p> <p>Syntax type: IA5 string</p> <p>RFC: Section 10 of Internet Draft http://search.ietf.org/internet-draft-lachman-ldap-mail-routing-03.txt.</p> <p><i>Note: A mailbox is needed by an account only if it uses the local delivery method. Accounts using forwarding delivery do not use a mailbox.</i></p>	mailUser
mailMTAFilter	<p>Flag to enable/disable SIEVE filtering of incoming messages by the MTA. This attribute can be used to prevent the delivery of unsolicited commercial e-mail (spam) to an account.</p> <p>Single or multiple value: Single, one of the following:</p> <ul style="list-style-type: none"> • 1 (enabled) • 0 (not enabled) <p>Default value: 0</p> <p>Matching rule: integerMatch</p> <p>Syntax type: Integer</p>	mailUserPrefs
mailMTAFilterPerUser	<p>Indication that a per-user filter is allowed.</p> <p>Single or multiple value: Single, one of the following:</p> <ul style="list-style-type: none"> • 1 (allowed) • 0 (not allowed) <p>Default value: 0</p> <p>Matching rule: integerMatch</p> <p>Syntax type: Integer</p>	mailUserPrefs

Attribute Name	Definition	Object Classes
mailParentalControl	<p>Flag to enable parental control for an account.</p> <p>Single or multiple value: Single, one of the following:</p> <ul style="list-style-type: none"> • 1 (parental control is enabled) • 0 (parental control is not enabled) <p>Default value: 1</p> <p>Matching rule: integerMatch</p> <p>Syntax type: Integer</p>	mailUserPrefs
mailPassword	<p>Password for the account login.</p> <p>Single or multiple value: Single</p> <p>Constraint: Maximum length is 64 characters.</p> <p>Matching rule: caseExactMatch</p> <p>Syntax type: Directory string</p>	mailUser
mailPasswordType	<p>Storage method in the directory for a mail password.</p> <p>Single or multiple value: Single, one of the following:</p> <ul style="list-style-type: none"> • C (clear, meaning the password is not encrypted) • M (Message Digest 5 (MD5) encryption) • U (standard UNIX encryption) • H (Secure Hash Algorithm (SHA1) encryption) • S (SHA1 with salt (SSHA1) encryption) • 1 (custom password type that allows you to implement your own hashing algorithm for passwords) • 2 (another custom password type) • 3 (another custom password type) • 4 (another custom password type) • 5 (another custom password type) <p>Matching rule: caseIgnoreMatch</p> <p>Syntax type: Printable string</p> <p><i>Note: This attribute should not be updated unless the mailPassword attribute is set at the same time.</i></p>	mailUser

Attribute Name	Definition	Object Classes
mailPOPAccess	<p>Flag to control account access to the standard POP3 service.</p> <p>Single or multiple value: Single, one of the following:</p> <p>all trusted none</p> <p>Default value: all</p> <p>Matching rule: caseIgnoreMatch</p> <p>Syntax type: Printable string</p>	mailUserPrefs
mailPOPProxyHost	<p>Host of an external POP server to which the mail system will proxy. Used during migration of accounts from one mail system to another.</p> <p>Single or multiple value: Single</p> <p>Constraint: Maximum length is 255 characters.</p> <p>Matching rule: caseIgnoreIA5Match</p> <p>Syntax type: IA5 string</p>	mailUser
mailPOPSSLAccess	<p>Flag enabling account access to the SSL-encrypted POP service.</p> <p>Single or multiple value: Single, one of the following:</p> <p>all trusted none</p> <p>Default value: all</p> <p>Matching rule: caseIgnoreMatch</p> <p>Syntax type: Printable string</p>	mailUserPrefs
mailQuotaBounceNotify	<p>Flag to control whether the MTA delivers a notification message to a mailbox when a message is rejected due to quota constraints.</p> <p>Single or multiple value: Single, one of the following:</p> <ul style="list-style-type: none"> • 1 (notification on) • 2 (notification off) <p>Default value: 1</p> <p>Matching rule: integerMatch</p> <p>Syntax type: Integer</p>	mailUserPrefs

Attribute Name	Definition	Object Classes
mailQuotaMaxMsgKB	<p>Maximum size, in kilobytes, of a message that can be accepted in an account's mailbox.</p> <p>Single or multiple value: Single</p> <p>Default value: 100</p> <p>Matching rule: integerMatch</p> <p>Syntax type: Integer</p>	mailUserPrefs
mailQuotaMaxMsgs	<p>Maximum number of messages that can exist in an account's mailbox.</p> <p>Single or multiple value: Single</p> <p>Default value: 1,000</p> <p>Matching rule: integerMatch</p> <p>Syntax type: Integer</p>	mailUserPrefs
mailQuotaThreshold	<p>Percentage of the mailbox quota that, when reached, triggers a warning notification to the user to delete some messages.</p> <p>Single or multiple value: Single, which can be a number from 0 to 100</p> <p>Default value: 70</p> <p>Matching rule: integerMatch</p> <p>Syntax type: Integer</p>	mailUserPrefs
mailQuotaTotKB	<p>Maximum message storage space, in kilobytes, in an account's mailbox.</p> <p>Single or multiple value: Single</p> <p>Default value: 10,000</p> <p>Matching rule: integerMatch</p> <p>Syntax type: Integer</p>	mailUserPrefs
mailRelayHost	<p>Name of another mail host to accept messages for a non-authoritative domain if the primary host does not recognize the recipient.</p> <p>Single or multiple value: Single</p> <p>Constraints:</p> <ul style="list-style-type: none"> • Used only if domainType is N. • Maximum length is 255 characters. <p>Matching rule: caseIgnoreIA5Match</p> <p>Syntax type: IA5 string</p>	mailDomain

Attribute Name	Definition	Object Classes
mailRewriteDomain	<p>New domain name for a recipient's e-mail address.</p> <p>Single or multiple value: Single</p> <p>Constraints:</p> <ul style="list-style-type: none"> • Used only if domainType is R. • Maximum length is 255 characters. <p>Matching rule: caseIgnoreMatch</p> <p>Syntax type: IA5 string</p> <p>Example: accordance.com would map to software.com if software.com were specified as the value of this attribute.</p>	mailDomain
mailSelfCare	<p>Flag enabling account access to the SelfCare Web interface. If it is set to 1, users can view and modify some of their account attributes.</p> <p>Single or multiple value: Single, one of the following:</p> <ul style="list-style-type: none"> • 1 (access enabled) • 0 (access not enabled) <p>Default value: 1</p> <p>Matching rule: integerMatch</p> <p>Syntax type: Integer</p>	mailUserPrefs
mailSelfCareSSL	<p>Flag enabling account access to the SSL-encrypted SelfCare Web interface.</p> <p>Single or multiple value: Single, one of the following:</p> <ul style="list-style-type: none"> • 1 (access enabled) • 0 (access not enabled) <p>Default value: 1</p> <p>Matching rule: integerMatch</p> <p>Syntax type: Integer</p>	mailUserPrefs

Attribute Name	Definition	Object Classes
mailSMTPAccess	<p>Flag enabling account access to the standard (unencrypted) SMTP service. Used only when mailSMTPAuth is enabled.</p> <p>Single or multiple value: Single, one of the following:</p> <ul style="list-style-type: none"> • 1 (access enabled) • 0 (access not enabled) <p>Default value: 1</p> <p>Matching rule: integerMatch</p> <p>Syntax type: Integer</p>	mailUserPrefs
mailSMTPAuth	<p>Flag controlling whether clients are required to authenticate themselves before sending mail through SMTP.</p> <p>Single or multiple value: Single, one of the following:</p> <ul style="list-style-type: none"> • 1 (authentication required) • 0 (authentication not required) <p>Default value: 0</p> <p>Matching rule: integerMatch</p> <p>Syntax type: Integer</p>	mailUserPrefs
mailSMTPRelayHost	<p>Host of an external SMTP server through which messages are to be relayed. Analogous to mailPOPProxyHost.</p> <p>Used during migration of accounts from one mail system to another.</p> <p>Single or multiple value: Single</p> <p>Constraint: Maximum length is 255 characters.</p> <p>Matching rule: caseIgnoreIA5Match</p> <p>Syntax type: IA5 string</p>	mailUser

Attribute Name	Definition	Object Classes
mailSMTPSSLAccess	<p>Flag enabling account access to the SSL-encrypted SMTP service. This attribute is meaningful only when mailSMTPAuth is set to 1.</p> <p>Single or multiple value: Single, one of the following:</p> <ul style="list-style-type: none"> • 1 (access enabled) • 0 (access not enabled) <p>Default value: 1</p> <p>Matching rule: integerMatch</p> <p>Syntax type: Integer</p>	mailUserPrefs
mailWebMailAccess	<p>Flag enabling account access to the WebEdge service.</p> <p>Single or multiple value: Single, one of the following:</p> <p>all trusted none</p> <p>Default value: all</p> <p>Matching rule: caseIgnoreMatch</p> <p>Syntax type: Printable string</p>	mailUserPrefs
mailWebMailAddressBookLimit	<p>Maximum number of address book entries that a user may define.</p> <p>Single or multiple value: Single</p> <p>Matching rule: integerMatch</p> <p>Syntax type: Integer</p>	mailUserPrefs
mailWebMailAddressBookListLimit	<p>Maximum number of e-mail addresses allowed in a single address book entry. This limits the size of personal distribution lists.</p> <p>Single or multiple value: Single</p> <p>Matching rule: integerMatch</p> <p>Syntax type: Integer</p>	mailUserPrefs

Attribute Name	Definition	Object Classes
mailWebMailAttachLimit	<p>Maximum number of file attachments that can be stored on the server while new messages are composed with the WebEdge client. When this limit is reached, the user must send or cancel a message.</p> <p>Single or multiple value: Single Matching rule: integerMatch Syntax type: Integer</p>	mailUserPrefs
mailWebMailAttachSizeLimit	<p>Maximum size of file attachments that can be sent through the WebEdge interface.</p> <p>Single or multiple value: Single Matching rule: integerMatch Syntax type: Integer</p>	mailUserPrefs
mailWebMailConfirmDelete	<p>Flag causing a prompt for confirmation to appear before a message is deleted in the WebEdge interface.</p> <p>Single or multiple value: Single, one of the following:</p> <ul style="list-style-type: none"> • 1 (prompt appears) • 0 (prompt does not appear) <p>Matching rule: integerMatch Syntax type: Integer</p>	mailUserPrefs
mailWebMailMsgAttachLimit	<p>Maximum number of files that can be attached to a single message in the WebEdge interface.</p> <p>Single or multiple value: Single Matching rule: integerMatch Syntax type: Integer</p>	mailUserPrefs
mailWebMailUseSignature	<p>Flag enabling automatic insertion of signature text at the end of a newly composed message.</p> <p>Single or multiple value: Single, one of the following:</p> <ul style="list-style-type: none"> • 1 (insertion enabled) • 0 (insertion not enabled) <p>Default value: 1 Matching rule: integerMatch Syntax type: Integer</p>	mailUserPrefs

Attribute Name	Definition	Object Classes
mailWildcardAccount	<p>An e-mail account within a mail domain that is to receive all mail sent to non-existent addresses within that domain.</p> <p>Single or multiple value: Single</p> <p>Constraints:</p> <ul style="list-style-type: none"> • Used only if domainType is L. • Maximum length is 64 characters. <p>Matching rule: caseIgnoreMatch</p> <p>Syntax type: IA5 string</p> <p>Example: If this attribute had a value of john.doe@software.com, any message sent to a non-existent address within software.com would be delivered to john.doe@software.com.</p>	mailDomain
manager	<p>Manager of an object represented by an entry.</p> <p>Single or multiple value: Multiple</p> <p>Matching rule: distinguishedNameMatch</p> <p>Syntax type: Distinguished name</p> <p>RFC: 1274 paragraph 9.3.10</p>	inetOrgPerson
matchingRules	<p>Single or multiple value: Multiple</p> <p>Matching rule: objectIdentifierFirstComponentMatch</p> <p>Syntax type: Matching rule</p> <p>RFC: 2252 paragraphs 4.5 and 5.1.8</p>	subschema
matchingRuleUse	<p>Single or multiple value: Multiple</p> <p>Matching rule: objectIdentifierFirstComponentMatch</p> <p>Syntax type: Matching rule use description</p> <p>RFC: 2252 paragraphs 5.1.9 and 6.19</p>	subschema
member	<p>Single or multiple value: Multiple</p> <p>Matching rule: distinguishedNameMatch</p> <p>Syntax type: Distinguished name, with:</p> <ul style="list-style-type: none"> • DN mapping • Attribute indexing • Enforcement of referential integrity <p>RFC: 2256 paragraph 5.32</p>	groupOfNames

Attribute Name	Definition	Object Classes
mobile	<p>Mobile telephone number associated with a person.</p> <p>Single or multiple value: Multiple, following the format for international telephone numbers.</p> <p>Matching rule: telephoneNumberMatch</p> <p>Syntax type: Telephone number</p> <p>Example: +44 71 123 4567</p> <p>RFC: 1274 paragraph 9.3.31</p>	inetOrgPerson
modifiersName	<p>Attribute associated with each entry, representing the distinguished name of the user who last modified the entry.</p> <p>Single or multiple value: Single</p> <p>Matching rule: distinguishedNameMatch</p> <p>Syntax type: Distinguished name, with:</p> <ul style="list-style-type: none"> • DN mapping <p>RFC: 2252 paragraph 5.1.4</p>	N/A (Directory operational attribute)
modifyTimestamp	<p>Attribute associated with each entry, representing the date and time the entry was last modified.</p> <p>Single or multiple value: Single</p> <p>Matching rule: generalizedTimeMatch</p> <p>Syntax type: Generalized time</p> <p>RFC: 2252 paragraph 5.1.2</p>	N/A (Directory operational attribute)
name	<p>Attribute supertype from which string attribute types typically used for naming are formed.</p> <p>Single or multiple value: Multiple</p> <p>Constraint: Maximum string length is 32,768 characters.</p> <p>Matching rule: caseIgnoreMatch</p> <p>Syntax type: Directory string</p> <p>RFC: 2256 paragraph 5.42</p>	N/A
nameForms	<p>Single or multiple value: Multiple</p> <p>Matching rule: objectIdentifierFirstComponentMatch</p> <p>Syntax type: Name form description</p> <p>RFC: 2252 paragraphs 5.4.2 and 6.22</p>	subschema

Attribute Name	Definition	Object Classes
newRDN	<p>New relative distinguished name (RDN) of an entry whose RDN was modified.</p> <p>Single or multiple value: Single</p> <p>Matching rule: distinguishedNameMatch</p> <p>Syntax type: Distinguished name</p>	changeLogEntry
newSuperior	<p>New parent of an entry whose relative distinguished name was modified.</p> <p>Single or multiple value: Single</p> <p>Matching rule: distinguishedNameMatch</p> <p>Syntax type: Distinguished name</p>	changeLogEntry
o	<p>Name of an organization.</p> <p>Single or multiple value: Multiple</p> <p>Matching rule: caseIgnoreMatch</p> <p>Syntax type: Directory string</p> <p>RFC: 2256 paragraph 5.11</p>	applicationEntity device domain groupOfNames groupOfUniqueNames inetOrgPerson organization
objectClass	<p>Description of the kind of object represented by an entry. This attribute is present in every entry with at least two values.</p> <p>Single or multiple value: Multiple, chosen from the following list:</p> <p>top</p> <p><any structural class name></p> <p>Matching rule: objectIdentifierMatch</p> <p>Syntax type: OID</p> <p>RFC: 2256 paragraph 5.1</p>	top
objectClasses	<p>Single or multiple value: Multiple</p> <p>Matching rule: objectIdentifierFirstComponentMatch</p> <p>Syntax type: Object class description</p> <p>RFC: 2252 paragraphs 4.4 and 5.1.7</p>	subschema

Attribute Name	Definition	Object Classes
ou	Name of an organizational unit, such as a department. Single or multiple value: Multiple Matching rule: caseIgnoreMatch Syntax type: Directory string RFC: 2256 paragraph 5.12	applicationEntity applicationProcess device groupOfNames groupOfUniqueNames organizationalPerson organizationalRole organizationalUnit
owner	Single or multiple value: Multiple Matching rule: caseIgnoreMatch Syntax type: Directory string RFC: 2256 paragraph 5.33	device groupOfNames groupOfUniqueNames
pager	Pager telephone number associated with a person. Single or multiple value: Multiple, each following the format for international telephone numbers. Single or multiple value: Multiple Matching rule: telephoneNumberMatch Syntax type: Telephone number Example: +44 71 123 4567 RFC: 1274 paragraphs 9.3.32	inetOrgPerson
partition	Definition of directory partitions. Single or multiple value: Multiple Matching rule: none Syntax type: Directory string	partition
partitionName	Attribute associated with each entry that is a member of a partition. Its value is the name of the partition. Single or multiple value: Multiple Matching rule: caseIgnoreMatch Syntax type: Directory string	N/A (Directory operational attribute)

Attribute Name	Definition	Object Classes
photo	<p>Specification of a photograph of a person. This should be encoded in G3 fax with ANS.1 wrapper.</p> <p>Single or multiple value: Multiple</p> <p>Matching rule: OctetStringMatch</p> <p>Syntax type: Octet string</p> <p>RFC: 1274 paragraph 9.3.7</p>	inetOrgPerson
physicalDeliveryOfficeName	<p>Single or multiple value: Multiple</p> <p>Constraint: Maximum string length is 128 characters.</p> <p>Matching rule: caseIgnoreMatch</p> <p>Syntax type: Directory string</p> <p>RFC: 2256 paragraph 5.20</p>	dmd domain organization organizationalPerson organizationalRole organizationalUnit residentialPerson
postalAddress	<p>Single or multiple value: Multiple</p> <p>Matching rule: caseIgnoreListMatch</p> <p>Syntax type: Postal address</p> <p>RFC: 2256 paragraph 5.17</p>	dmd domain organization organizationalPerson organizationalRole organizationalUnit residentialPerson
postalCode	<p>Single or multiple value: Multiple</p> <p>Constraint: Maximum string length is 40 characters.</p> <p>Matching rule: caseIgnoreMatch</p> <p>Syntax type: Directory string</p> <p>RFC: 2256 paragraph 5.18</p>	dmd domain organization organizationalPerson organizationalRole organizationalUnit residentialPerson
postOfficeBox	<p>Single or multiple value: Multiple</p> <p>Constraint: Maximum string length is 40 characters.</p> <p>Matching rule: caseIgnoreMatch</p> <p>Syntax type: Directory string</p> <p>RFC: 2256 paragraph 5.19</p>	dmd domain organization organizationalPerson organizationalRole organizationalUnit residentialPerson
preferredDeliveryMethod	<p>Single or multiple value: Single</p> <p>Matching rule: caseIgnoreMatch</p> <p>Syntax type: Delivery method</p> <p>RFC: 2256 paragraph 5.29</p>	dmd domain organization organizationalPerson organizationalRole organizationalUnit residentialPerson

Attribute Name	Definition	Object Classes
preferredLanguage	<p>Preferred written or spoken language for a person.</p> <p>Single or multiple value: Single</p> <p>Matching rule: caseIgnoreMatch</p> <p>Syntax type: Directory string</p> <p>RFC: Draft-smith-ldap-inetorgperson-03; paragraph 5.7</p>	inetOrgPerson
presentationAddress	<p>An OSI (Open Systems Interconnection) presentation address.</p> <p>Single or multiple value: Single</p> <p>Matching rule: presentationAddressMatch</p> <p>Syntax type: Presentation address</p> <p>RFC: 2256 paragraph 5.30</p>	applicationEntity
registeredAddress	<p>Postal address suitable for receipt of telegrams or documents for which the recipient must accept delivery.</p> <p>Single or multiple value: Multiple</p> <p>Matching rule: caseIgnoreListMatch</p> <p>Syntax type: Postal address</p> <p>RFC: 2256 paragraph 5.27</p>	dmd domain organization organizationalPerson organizationalRole organizationalUnit residentialPerson

Attribute Name	Definition	Object Classes
replArea	<p>Objects and attributes to be replicated to the consumer server (Directory Cache server). These are specified using three configuration keys: <code>replAreaSpec</code>, <code>partition</code>, and <code>attributeSelection</code>. These configuration keys are discussed in Chapter 8.</p> <p>You construct the replication area specification by specifying an attribute group name and a partition name.</p> <p>You specify a partition by specifying the root of a subtree. All objects in that subtree are part of the partition. Use an LDAP filter to specify a smaller subset of objects.</p> <p>You can replicate either a complete or partial object. Select attributes by specifying an <code>INCLUDE</code> or <code>EXCLUDE</code> list in the <code>attributeSelection</code> configuration key.</p> <p>If an object does not satisfy any replication area specification, it is not replicated to a Directory Cache server.</p> <p>If no replication area attribute is present in a replication agreement, all objects and attributes are replicated.</p> <p>Single or multiple value: Multiple Matching rule: none Syntax type: Directory string</p> <p><i>Caution! The replication area specification must pull all the required non-leaf nodes (nodes that have descendents). Otherwise, replication for leaf nodes would fail.</i></p>	replAgreement
roleOccupant	<p>Single or multiple value: Multiple Matching rule: distinguishedNameMatch Syntax type: Distinguished name RFC: 2256 paragraph 5.34</p>	organizationalRole
roomNumber	<p>Room number of an object.</p> <p>Single or multiple value: Multiple Constraint: Maximum string length is 256 characters. Matching rule: caseIgnoreMatch Syntax type: Directory string RFC: 1274 paragraph 9.3.6</p>	inetOrgPerson

Attribute Name	Definition	Object Classes
scAttributeIndexInfo	<p>Single or multiple value: Multiple</p> <p>Matching rule: caseIgnoreMatch</p> <p>Syntax type: Printable string</p> <p><i>Note: For Software.com internal use only.</i></p>	scConfig
scCacheDirDbStatus	<p>Single or multiple value: Single</p> <p>Matching rule: caseIgnoreMatch</p> <p>Syntax type: Printable string</p> <p><i>Note: For Software.com internal use only.</i></p>	scConfigRoot
scSchemaFileTimestamp	<p>Single or multiple value: Single</p> <p>Matching rule: generalizedTimeMatch</p> <p>Syntax type: Generalized time</p> <p><i>Note: For Software.com internal use only.</i></p>	scSubschema
secretary	<p>Secretary of a person.</p> <p>Single or multiple value: Multiple, each of which is a distinguished name</p> <p>Matching rule: distinguishedNameMatch</p> <p>Syntax type: Distinguished name</p> <p>RFC: 1274 paragraph 9.3.17</p>	inetOrgPerson
seeAlso	<p>Single or multiple value: Multiple</p> <p>Matching rule: distinguishedNameMatch</p> <p>Syntax type: Distinguished name</p> <p>RFC: 2256 paragraph 5.35</p>	applicationEntity applicationProcess device dmd domain groupOfNames groupOfUniqueNames locality organization organizationalRole organizationalUnit person
serialNumber	<p>Serial number of a device.</p> <p>Single or multiple value: Multiple</p> <p>Constraint: Maximum string length is 64 characters.</p> <p>Matching rule: caseIgnoreMatch</p> <p>Syntax type: Printable string</p> <p>RFC: 2256 paragraph 5.6</p>	device

Attribute Name	Definition	Object Classes
sn	<p>Family name (surname) of a person.</p> <p>Single or multiple value: Single</p> <p>Matching rule: caseIgnoreMatch</p> <p>Syntax type: Directory string</p> <p>Example: Smith</p> <p>RFC: 2256 paragraph 5.5</p>	person
st	<p>Full name of a state or province.</p> <p>Single or multiple value: Multiple</p> <p>Constraint: Maximum string length is 128 characters.</p> <p>Matching rule: caseIgnoreMatch</p> <p>Syntax type: Directory string</p> <p>RFC: 2256 paragraph 5.9</p>	dmd domain locality organization organizationalPerson organizationalRole organizationalUnit residentialPerson
street	<p>Physical address of the object to which the entry corresponds.</p> <p>Single or multiple value: Multiple</p> <p>Matching rule: caseIgnoreMatch</p> <p>Syntax type: Directory string</p> <p>RFC: 2256 paragraph 5.10</p>	dmd domain locality organization organizationalPerson organizationalRole organizationalUnit residentialPerson
supplierReference	<p>Supplier (Directory server) host and LDAP port number. The consumer server (Directory Cache server) binds to this supplier server to read change logs.</p> <p>Single or multiple value: Single</p> <p>Default value: The first name on the list of hosts in the ldapMasterHosts configuration parameter of the Directory Cache server</p> <p>Matching rule: none</p> <p>Syntax type: IA5 string</p> <p>Example: ldap://abc.isp.com:5004</p>	replAgreement

Attribute Name	Definition	Object Classes
supportedAlgorithms	<p>This attribute is to be stored and requested in binary form, as <code>supportedAlgorithms;binary</code>.</p> <p>Single or multiple value: Multiple</p> <p>Matching rule: none</p> <p>Syntax type: Supported algorithm</p> <p>RFC: 2256 paragraph 5.53</p>	userSecurityInformation
supportedApplicationContext	<p>Identifiers of OSI (Open Systems Interconnection) application contexts.</p> <p>Single or multiple value: Multiple</p> <p>Matching rule: objectIdentifierMatch</p> <p>Syntax type: OID</p> <p>RFC: 2256 paragraph 5.31</p>	applicationEntity
targetDN	<p>Distinguished name of a modified entry.</p> <p>Single or multiple value: Single</p> <p>Matching rule: distinguishedNameMatch</p> <p>Syntax type: Distinguished name</p>	changeLogEntry
telephoneNumber	<p>Telephone number for a user.</p> <p>Single or multiple value: Multiple</p> <p>Constraint: Maximum length is 32 characters.</p> <p>Matching rule: telephoneNumberMatch</p> <p>Syntax type: Telephone number</p> <p>RFC: 2256 paragraph 5.21</p>	dmd domain organization organizationalPerson organizationalRole organizationalUnit person residentialPerson
teletexTerminalIdentifier	<p>Single or multiple value: Multiple</p> <p>Matching rule: none</p> <p>Syntax type: Telex terminal identifier</p> <p>RFC: 2256 paragraph 5.23</p>	dmd domain organization organizationalPerson organizationalRole organizationalUnit residentialPerson
telexNumber	<p>Single or multiple value: Multiple</p> <p>Matching rule: none</p> <p>Syntax type: Telex number</p> <p>RFC: 2256 paragraph 5.22</p>	dmd domain organization organizationalPerson organizationalRole organizationalUnit residentialPerson

Attribute Name	Definition	Object Classes
title	<p>Job description title of a person.</p> <p>Single or multiple value: Multiple</p> <p>Matching rule: caseIgnoreMatch</p> <p>Syntax type: Directory string</p> <p>Example: Vice-President</p> <p>RFC: 2256 paragraph 5.13</p>	organizationalPerson
uid	<p>User's login name.</p> <p>Single or multiple value: Multiple</p> <p>Constraint: Maximum length is 256 characters.</p> <p>Matching rule: caseIgnoreMatch</p> <p>Substrings matching rule: caseIgnoreSubstringsMatch</p> <p>Syntax type: Directory string</p> <p>RFC: 1274 paragraph 9.3.1</p>	inetOrgPerson
uniqueMember	<p>Single or multiple value: Multiple</p> <p>Matching rule: uniqueMemberMatch</p> <p>Syntax type: Name and optional UID</p> <p>RFC: 2256 paragraph 5.51</p>	groupOfUniqueNames
updateInterval	<p>Update interval in seconds. This update thread in the Directory Cache server runs at this interval to read changes from the supplier server. It replicates these changes in its local Directory Cache database according to the replication area specification in replArea.</p> <p>Single or multiple value: Single</p> <p>Matching rule: integerMatch</p> <p>Syntax type: Integer</p>	replAgreement

Attribute Name	Definition	Object Classes
userCertificate	<p>Certified public key of the user; this key is used for authentication and encryption/decryption.</p> <p>This attribute is to be stored and requested in binary form, as <code>userCertificate;binary</code>.</p> <p>Single or multiple value: Multiple</p> <p>Matching rule: none</p> <p>Syntax type: Certificate</p> <p>RFC: 2256 paragraph 5.37</p>	inetOrgPerson
userPassword	<p>Password for a user.</p> <p>Single or multiple value: Multiple</p> <p>Constraint: Maximum string length is 128 characters.</p> <p>Matching rule: <code>octetStringMatch</code></p> <p>Syntax type: Octet string</p> <p>RFC: 2256 paragraph 5.36</p>	dmd domain organization organizationalPerson organizationalUnit
userPKCS12	<p>Format for the exchange of personal identity information.</p> <p>Single or multiple value: Multiple</p> <p>Matching rule: none</p> <p>Syntax type: Octet string</p> <p>RFC: Draft-smith-ldap-inetorgperson-03; paragraph 5.9</p>	inetOrgPerson
userSMIMECertificate	<p>Signed message used to support S/MIME. It contains the person's certificate chain and algorithm capabilities, stored as binary data.</p> <p>Single or multiple value: Multiple</p> <p>Matching rule: none</p> <p>Syntax type: Octet string</p> <p>RFC: Draft-smith-ldap-inetorgperson-03; paragraph 5.8</p>	inetOrgPerson
x121Address	<p>Single or multiple value: Multiple</p> <p>Constraint: Maximum string length is 15 characters</p> <p>Matching rule: <code>numericStringMatch</code></p> <p>Syntax type: Numeric string</p> <p>RFC: 2256 paragraph 5.25</p>	dmd domain organization organizationalPerson organizationalRole organizationalUnit residentialPerson

Attribute Name	Definition	Object Classes
x500UniqueIdentifier	<p>Flag used to distinguish between objects if a distinguished name (DN) has been used more than once.</p> <p>Single or multiple value: Multiple</p> <p>Matching rule: bitStringMatch</p> <p>Syntax type: Bit string</p> <p>RFC: 2256 paragraph 5.46</p>	inetOrgPerson

8

Directory Configuration Keys

You can customize the behavior of the Directory server and Directory Cache server using the configuration keys described in this chapter.

Note: For a detailed discussion of configuration management and instructions on changing configuration keys, see Chapter 4 of the *InterMail Mx Operations Guide*.

This chapter contains the following:

- A sample configuration key description, with an explanation of terminology
- An alphabetical listing of all configuration keys for the Directory server and the Directory Cache server

Sample Configuration Key

The table for the fictional configuration key `configKeyName` introduces the table format and terminology used throughout this chapter.

Note: Although multi-word keys appear written in both upper and lowercase, this is solely for the sake of readability. All configuration keys are case-insensitive.

configKeyName

Description: Explains the purpose of the key, describes the format of key entries, and provides suggested settings where appropriate.

Related Keys: Lists additional configuration keys (if any) that work together with this key to achieve a specific result.

Servers Affected: Indicates the InterMail servers affected by this key.

- Change Impact:** Describes the implications of changing the value of this configuration key. The possible impacts are:
- Server restart required
 - Trivial, no server restart required
 - No impact on server
- For descriptions of these impacts, see “Impact of Configuration Key Changes” on page 187.
- Possible Values:** Describes the allowable values for a key, such as `true` or `false`, a text string, an integer, and so forth.
- Initial Value:** Defines the entry for a configuration key initially set in the `config.db` file during InterMail installation.
- Default Value:** Specifies the value the system inserts if there is no explicit value set for this particular key. The default value is hard-coded in the `config.db` file.
- If several servers use the same configuration key, there may be different default settings for each server.
- “Null” designates the absence of a value.
- Example:** Sample syntax for the key, including the complete configuration hierarchy, the key name, a colon, a space, and the value of the key enclosed in square brackets. For example:
- ```
/*/mta/configKeyName: [true]
```

## InterMail Servers and Processes

Each InterMail server has a corresponding process name. Unless otherwise indicated, the syntax for each configuration key must include the appropriate server process name. For example, in the following key the checkpoint interval on the Directory Cache server (`imdircacheserv`) is set to 1 second:

```
/*/imdircacheserv/checkPointInterval: [1]
```

The InterMail servers and their corresponding server process names are as follows:

| Server Name                   | Server Process Name         |
|-------------------------------|-----------------------------|
| MTA (Message Transport Agent) | <code>mta</code>            |
| MSS (Message Store Server)    | <code>mss</code>            |
| POP server                    | <code>popserv</code>        |
| IMAP server                   | <code>imapserv</code>       |
| Directory Cache server        | <code>imdircacheserv</code> |

| Server Name          | Server Process Name |
|----------------------|---------------------|
| Directory server     | imdirserv           |
| Configuration server | imconfserv          |
| Manager server       | immgrserv           |
| Queue server         | imqueueserv         |
| SNMP server          | snmpdm              |
| WebEdge server       | webedge             |

You can also use the `sysadmin` module in place of the server process name for certain configuration settings. When this is the case, the example indicates it clearly.

### Common Server Configuration

Some configuration keys can define settings for more than one server at a time. Where indicated, you can use `common` in place of server process names to use a single setting to configure every server affected by this particular key.

For example, the `dirRmeConnections` key, which sets the number size of the connection pool between the Directory Cache server and the other InterMail servers, can apply to both the Directory and Directory Cache servers. You can define the size for both servers with a single command by using `common` in place of the process name, as follows:

```
/*/common/dirRmeConnections: [40]
```

### Individual Server Configuration

If there is a requirement to have different sizes for the Directory and Directory Cache servers, set them independently, as follows:

```
/*/imdirserv/dirRmeConnections: [40]
```

```
/*/imdircacheserv/dirRmeConnections: [60]
```

## Impact of Configuration Key Changes

The Change Impact section of the configuration key table describes the implications of changing the value of a particular configuration key. The possible impacts are:

- **Server restart required**—You must restart the server for the change you made to take effect. The server can read the new setting only at startup time. The server does not restart automatically; you must restart it.
- **Trivial, no server restart required**—The server will be able to read the new configuration setting the next time it is necessary without having to be restarted first.

- **No impact on server**—Changing the value of the configuration key affects something other than a server, typically a utility that retrieves the new value the next time it runs.

## Directory Configuration Keys

The following is a list of all directory-related configuration keys that you can set in the Configuration database (`config.db`).

---

**Caution!** Certain configuration keys in this section allow you to specify a single IP address or a list of IP addresses. When specifying IP addresses as values for these keys, be aware that 0 signifies a wildcard. For example, specifying 0.0.0.0 as a value for the `relaySourceRemoteIPList` allows anyone to relay.

0.0.0.0 is not a valid alias for the local host, and it should not be used as such. 127.0.0.1 should always be used instead.

---

### anonBindAccess

**Description:** Determines which users can have anonymous bind access, which allows them to log in and authenticate without providing a password.

If `All`, all users have anonymous bind access.

If `Trusted`, users logging in from a trusted IP address have anonymous bind access. If using this value, you must set the value of the configuration key `trustedInterfaces` to a list of trusted IP addresses.

If `None`, anonymous bind access is not allowed for any user.

**Related Keys:** `trustedInterfaces`

**Servers Affected:** Directory server and Directory Cache server

**Change Impact:** trivial, no server restart required

**Possible Values:** All  
Trusted  
None

**Initial Value:** none

**Default Value:** none

**Example:** `/*/imdircachserv/anonBindAccess: [none]`

## attributeAliasingEnable

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description:</b>      | Is a flag that enables you to use an alias for the name of a Directory database attribute. This is useful if your application has a different name for an attribute that has the same function as an InterMail Directory database attribute.<br><br>For example, assume your application uses an attribute <code>userLogin</code> with the same functionality as the InterMail attribute <code>mailLogin</code> . You could set this key to <code>true</code> to bring up an aliasing table in which you would enter these two attributes. The InterMail system would then read <code>userLogin</code> as equivalent to <code>mailLogin</code> . |
| <b>Related Keys:</b>     | none                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Servers Affected:</b> | Directory server, Directory Cache server                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Change Impact:</b>    | trivial, no server restart required                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Possible Values:</b>  | <code>true</code><br><code>false</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Initial Value:</b>    | <code>false</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Default Value:</b>    | <code>false</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Example:</b>          | <code>/*/imdirserv/attributeAliasingEnable: [false]</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

## attributeSelection

|                          |                                                                                                                                                                 |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description:</b>      | Groups together attributes used by a specific directory application. This key is used to select particular attributes during replication.                       |
| <b>Related Keys:</b>     | <code>partition</code> , <code>replAreaSpec</code> , <code>ldapReplicationAgreement</code>                                                                      |
| <b>Servers Affected:</b> | Directory Cache server                                                                                                                                          |
| <b>Change Impact:</b>    | server restart required                                                                                                                                         |
| <b>Possible Values:</b>  | <code>&lt;attribute group name&gt; :: include   exclude<br/>(* &lt;attribute name1&gt; \$ &lt;attribute name2&gt; \$<br/>&lt;attribute name3&gt; \$ ...)</code> |
| <b>Initial Value:</b>    |                                                                                                                                                                 |
| <b>Default Value:</b>    | No groupings                                                                                                                                                    |

**Example:**

```
/*/imdircachserv/attributeSelection:
[wp_attrs :: include (objectclass $ cn $ sn $
givenName $ street $ mail $ telephoneNumber)]
```

## cacheAlwaysReadThru

**Description:** Specifies whether the Directory Cache server always reads through to the Integrated Services Directory when looking for account information instead of first reading from the local cache.

If `true`, the Directory Cache server reads through to the Integrated Services Directory instead of first reading from the local cache.

If `false`, the Directory Cache server functions as normal and only reads through to the Integrated Services Directory if it cannot locate the needed information in its local cache first.

***Note:** This key does not supersede and is not superseded by the configuration key `cacheDisableReadThrus`. If both keys are set to `true`, the Directory Cache server always responds with `MS_UNKNOWNUSER`.*

**Related Keys:** `cacheDisableReadThrus`

**Servers Affected:** Directory Cache server

**Change Impact:** trivial, no server restart required

**Possible Values:** `true`  
`false`

**Initial Value:** `false`

**Default Value:** `false`

**Example:**

```
/*/imdircachserv/cacheAlwaysReadThru: [false]
```

## cacheAuthoritativeForMTA

**Description:** Specifies whether information in the Directory Cache database is considered authoritative for account queries from the MTA.

If the setting is `false` and the Directory Cache server does not find requested information in its local cache file, the server attempts to read through to the Directory server to obtain the necessary information.

If the setting is `true`, cached information is considered authoritative, and no attempt is made to read through to the Directory server.

---

|                          |                                                                   |
|--------------------------|-------------------------------------------------------------------|
| <b>Related Keys:</b>     | cacheAuthoritativeOnDbFail                                        |
| <b>Servers Affected:</b> | Directory Cache server                                            |
| <b>Change Impact:</b>    | trivial, no server restart required                               |
| <b>Possible Values:</b>  | true<br>false                                                     |
| <b>Initial Value:</b>    | false                                                             |
| <b>Default Value:</b>    | false                                                             |
| <b>Example:</b>          | <pre>/*/imdircachserv/cacheAuthoritativeForMTA:<br/>[false]</pre> |

## cacheAuthoritativeOnDbFail

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description:</b>      | <p>Specifies whether the Directory Cache server is considered authoritative or non-authoritative.</p> <p>If it is authoritative, it operates independently of the Directory server, even when lookups fail in its local Directory Cache database.</p> <p>If it is non-authoritative, a lookup failure results in a read-through to the Directory server to search for the information in the master Directory database.</p> |
| <b>Related Keys:</b>     | cacheAuthoritativeForMTA, cacheDisableReadThrus, cacheDisableWriteThrus                                                                                                                                                                                                                                                                                                                                                     |
| <b>Servers Affected:</b> | Directory Cache server                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Change Impact:</b>    | trivial                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Possible Values:</b>  | true<br>false                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Initial Value:</b>    | true                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Default Value:</b>    | true                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Example:</b>          | <pre>/*/imdircachserv/cacheAuthoritativeOnDbFail:<br/>[true]</pre>                                                                                                                                                                                                                                                                                                                                                          |

## cacheDisableReadThrus

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description:</b>      | <p>Specifies whether read-throughs to the master Directory database are disabled, causing the Directory Cache server to be the authoritative source of information.</p> <p>Under normal circumstances, the Directory Cache server reads through to the Directory server if it cannot find a particular user or the proper password in its local cache. However, if a large number of users or passwords cannot be located, CPU resources may be drained. If this is a problem in your environment, you may want to consider disabling read-throughs.</p> <p>If this key is set to <code>true</code>, no read-throughs to the Directory server take place. If this key is set to <code>false</code>, the Directory Cache server functions as normal.</p> <p>This key takes precedence over the <code>cacheAuthoritativeForMTA</code> and <code>cacheAuthoritativeOnDbFail</code> configuration keys.</p> |
| <b>Related Keys:</b>     | <code>cacheAlwaysReadThru</code> , <code>cacheAuthoritativeOnDbFail</code> , <code>cacheAuthoritativeForMTA</code> , <code>cacheDisableWriteThrus</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Servers Affected:</b> | Directory Cache Server                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Change Impact:</b>    | No read-throughs to the Directory server take place when this key is set to <code>true</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Possible Values:</b>  | <code>true</code><br><code>false</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Initial Value:</b>    | <code>false</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Default Value:</b>    | <code>false</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Example:</b>          | <code>/*/imdircacheserv/cacheDisableReadThrus: [false]</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

## cacheDisableWriteThrus

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description:</b>      | <p>Specifies whether write-throughs to the master Directory database are disabled, causing the Directory Cache server to be the authoritative source of information.</p> <p>Under normal circumstances, the Directory Cache Server writes through to the Directory server if it cannot find a particular user or the proper password in its local cache. However, if a large number of users or passwords cannot be located, CPU resources may be drained. If this is a problem in your environment, you may want to consider disabling write-throughs.</p> <p>If this key is set to <code>true</code>, no write-throughs to the Directory server take place. If this key is set to <code>false</code>, the Directory Cache server functions as normal.</p> |
| <b>Related Keys:</b>     | <code>cacheDisableReadThrus</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Servers Affected:</b> | Directory Cache Server                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Change Impact:</b>    | No write-throughs to the Directory server take place when this key is set to <code>true</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Possible Values:</b>  | <code>true</code><br><code>false</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Initial Value:</b>    | <code>false</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Default Value:</b>    | <code>false</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Example:</b>          | <pre>/*/imdircachesserv/cacheDisableWriteThrus: [false]</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

## cacheReReadInterval

|                          |                                                                                                                                                                                                               |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description:</b>      | <p>Specifies the number of seconds the system is to wait before checking to see if the cache needs to be switched. The cache needs to be switched if <code>imdirsync</code> is run to create a new cache.</p> |
| <b>Related Keys:</b>     | <code>none</code>                                                                                                                                                                                             |
| <b>Servers Affected:</b> | Directory Cache server                                                                                                                                                                                        |
| <b>Change Impact:</b>    | trivial                                                                                                                                                                                                       |
| <b>Possible Values:</b>  | Any number from 1 to 3600, in seconds                                                                                                                                                                         |
| <b>Initial Value:</b>    | <code>none</code>                                                                                                                                                                                             |

**Default Value:** 5

**Example:** `/*/imdircachesserv/cacheReReadInterval: [10]`

## chainingInfo

**Description:** Provides the names of Directory Cache servers to be contacted by an index Directory Cache server to answer a request from an RME client. Maps the replication area specification specified by `replAreaSpec` to the host serving that specification.

**Related Keys:** `replAreaSpec`

**Servers Affected:** Directory Cache server

**Change Impact:** server restart required

**Possible Values:** [`<replAreaSpec name>: <hostname of first Directory Cache server>, <hostname of second Directory Cache server>`]

**Initial Value:**

**Default Value:** no chaining info

**Example:** `/*/imdircachesserv/chainingInfo:  
[MTA_WEST_INDEX: HOST_MTA_WEST, Host-Backup]`

## changeLog

**Description:** Specifies the distinguished name where the change log entries are stored.

***Caution!** Do not change this key once you have set up your database. You could lose changes that are in the old change log.*

**Related Keys:** `ldapBackend`

**Servers Affected:** Directory server

**Change Impact:** server restart required

**Possible Values:** Any valid distinguished name

**Initial Value:** `cn=changelog`

**Default Value:** `cn=changelog`

**Example:** `/*/imdirserv/changelog: [cn=changelog]`

## checkPointInterval

**Description:** Specifies the time interval, in seconds, between runs of the checkpoint thread.  
Data is written to the disk at these intervals so that it will be available in the event of a server crash.

**Related Keys:** none

**Servers Affected:** Directory Cache server

**Change Impact:** trivial

**Possible Values:** Between 1 and 60

**Initial Value:** 1

**Default Value:** 1

**Example:** `/*/imdircachserv/checkPointInterval: [1]`

## checkPointRetryInterval

**Description:** Represents the number of seconds the system should wait before retrying a checkpoint that has failed (typically, when `txn_checkpoint` returns `DB_INCOMPLETE`).

**Related Keys:** `checkPointInterval`

**Servers Affected:** Directory Cache server

**Change Impact:** trivial, no server restart required

**Possible Values:** Between 1 and 3600

**Initial Value:** 1

**Default Value:** 1

**Example:** `/*/imdircachserv/checkPointRetryInterval: [1]`

## chgLogPageSize

|                          |                                                                              |
|--------------------------|------------------------------------------------------------------------------|
| <b>Description:</b>      | Defines the number of entries to be read from the change log at one time.    |
| <b>Related Keys:</b>     | none                                                                         |
| <b>Servers Affected:</b> | Directory Cache server                                                       |
| <b>Change Impact:</b>    | trivial                                                                      |
| <b>Possible Values:</b>  | Any numeric value less than the value of the configuration key ldapSizeLimit |
| <b>Initial Value:</b>    | 499                                                                          |
| <b>Default Value:</b>    | 100                                                                          |
| <b>Example:</b>          | <code>/*/imdircacheserv/chgLogPageSize: [100]</code>                         |

## compatibleQuotaKbytesConversion

|                          |                                                                              |
|--------------------------|------------------------------------------------------------------------------|
| <b>Description:</b>      | Determines the conversion factor the system uses to convert Kbytes to bytes. |
| <b>Related Keys:</b>     | none                                                                         |
| <b>Servers Affected:</b> | IMAP, MSS, MTA, POP, Directory Cache server                                  |
| <b>Change Impact:</b>    | trivial, no server restart required                                          |
| <b>Possible Values:</b>  | true<br>false                                                                |
| <b>Initial Value:</b>    | false                                                                        |
| <b>Default Value:</b>    | false                                                                        |
| <b>Example:</b>          | <code>/*/common/compatibleQuotaKbytesConversion: [false]</code>              |

## createEntryAudit

|                     |                                                                                                                                                       |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description:</b> | Is a flag that indicates whether operational attributes (createTimestamp and creatorsName) are to be created for audit purposes for every LDAP entry. |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|

|                          |                                                    |
|--------------------------|----------------------------------------------------|
| <b>Related Keys:</b>     | none                                               |
| <b>Servers Affected:</b> | Directory server                                   |
| <b>Change Impact:</b>    | trivial                                            |
| <b>Possible Values:</b>  | true<br>false                                      |
| <b>Initial Value:</b>    | none                                               |
| <b>Default Value:</b>    | true                                               |
| <b>Example:</b>          | <code>/*/imdirserv/createEntryAudit: [true]</code> |

## dbLogFileMaxSizeKb

|                          |                                                                                    |
|--------------------------|------------------------------------------------------------------------------------|
| <b>Description:</b>      | Defines the maximum size of a database log file, which is used for crash recovery. |
| <b>Related Keys:</b>     | none                                                                               |
| <b>Servers Affected:</b> | MSS, Directory Cache server                                                        |
| <b>Change Impact:</b>    | server restart required                                                            |
| <b>Possible Values:</b>  | Any non-negative integer                                                           |
| <b>Initial Value:</b>    | 64                                                                                 |
| <b>Default Value:</b>    | 64                                                                                 |
| <b>Example:</b>          | <code>/*/mss/dbLogFileMaxSizeKb: [64]</code>                                       |

## dbSuppressFsync

|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description:</b>  | <p>Controls whether the cache files and cache file logs will synchronize when modified.</p> <p>If this key is set to <code>true</code> (the default), the files will not synchronize. This setting provides better performance.</p> <p>If this key is set to <code>false</code>, there is less chance that the cache files will be corrupted if the machine on which the Directory Cache server is running crashes. However, if the files are corrupted, use <code>imdirsync</code> to regenerate them.</p> |
| <b>Related Keys:</b> | none                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

**Servers Affected:** Directory Cache server

**Change Impact:** trivial

**Possible Values:** true  
false

**Initial Value:** true

**Default Value:** false

**Example:** `/*/imdircachesserv/dbSupressFsync: [true]`

## defaultBindDN

**Description:** Specifies the distinguished name used by tools such as `imdbcontrol` and the C API that cannot bind to the LDAP server but need to communicate with the Directory Cache server.

**Related Keys:** `defaultBindPassword`

**Servers Affected:** Directory Cache server

**Change Impact:** server restart required

**Possible Values:** Any distinguished name value

**Initial Value:** `[]`

**Default Value:** `cn=root`

**Example:** `/*/imdirserv/defaultBindDN: [cn=root]`

## defaultBindPassword

**Description:** Specifies the password used with the configuration key `defaultBindDN`.

**Related Keys:** `defaultBindDN`

**Servers Affected:** Directory Cache server

**Change Impact:** server restart required

**Possible Values:** Any alphanumeric string with or without special characters

**Initial Value:** `[]`

**Default Value:** `secret` (randomly generated string of uppercase characters)

**Example:** `/*/imdirserv/defaultBindPassword: [secret]`

## defaultChangelogTablespace

**Description:** Indicates that IM\_CHGLG\_YYYYMMDDHHMMSS tables are to be stored in a tablespace other than the one installed by the InterMail Oracle installation utility.

**Related Keys:** `defaultChangelogIndexTablespace`

**Servers Affected:** Directory server

**Change Impact:** trivial, no server restart required

**Possible Values:** Any string

**Initial Value:** none

**Default Value:** CHANGELOG

**Example:** `/*/imdirserv/defaultChangelogTablespace: [CHANGELOG]`

## defaultDirServer

**Description:** Specifies the LDAP server (either the Directory Cache server or the Directory server) to which imdbcontrol connects if the host and port are not specified on the command line.  
This is an imdbcontrol key.

**Related Keys:** none

**Servers Affected:** Directory server, Directory Cache server

**Change Impact:** none

**Possible Values:** Configuration name of any LDAP server: imdirserv or imdircacheserv

**Initial Value:** imdirserv

**Default Value:** imdirserv

**Example:** `/*/imdbcontrol/defaultDirServer: [imdirserv]`

## dirCachePort

|                          |                                                                                                                                                                                                                                                                                                   |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description:</b>      | Defines the port number on which the Directory Cache server listens for RME requests.<br>To support failover, it is advisable that each Directory Cache server have a different port number. This enables you to run two virtual hosts on a single system without creating port number conflicts. |
| <b>Related Keys:</b>     | none                                                                                                                                                                                                                                                                                              |
| <b>Servers Affected:</b> | Directory Cache Server                                                                                                                                                                                                                                                                            |
| <b>Change Impact:</b>    | server restart required                                                                                                                                                                                                                                                                           |
| <b>Possible Values:</b>  | Any valid, unused port number                                                                                                                                                                                                                                                                     |
| <b>Initial Value:</b>    | Set during installation                                                                                                                                                                                                                                                                           |
| <b>Default Value:</b>    | null                                                                                                                                                                                                                                                                                              |
| <b>Example:</b>          | <code>/*/imdircacheserv/dirCachePort: [5888]</code>                                                                                                                                                                                                                                               |

## dirRmeConnections

|                          |                                                                                                               |
|--------------------------|---------------------------------------------------------------------------------------------------------------|
| <b>Description:</b>      | Specifies the size of the connection pool between the Directory Cache server and the other InterMail servers. |
| <b>Related Keys:</b>     | none                                                                                                          |
| <b>Servers Affected:</b> | Directory server, Directory Cache server                                                                      |
| <b>Change Impact:</b>    | server restart required                                                                                       |
| <b>Possible Values:</b>  | Any integer from 1 to 512                                                                                     |
| <b>Initial Value:</b>    | 40                                                                                                            |
| <b>Default Value:</b>    | 10                                                                                                            |
| <b>Example:</b>          | <code>/*/common/dirRmeConnections: [40]</code>                                                                |

## dirRmeHost

|                     |                                                                                                              |
|---------------------|--------------------------------------------------------------------------------------------------------------|
| <b>Description:</b> | Specifies the name of the host running the Directory Cache server in builds using only one Directory server. |
|---------------------|--------------------------------------------------------------------------------------------------------------|

|                          |                                     |
|--------------------------|-------------------------------------|
| <b>Related Keys:</b>     | ldapServerHosts                     |
| <b>Servers Affected:</b> | Directory Cache server              |
| <b>Change Impact:</b>    | trivial, no server restart required |
| <b>Possible Values:</b>  | Any valid host name                 |
| <b>Initial Value:</b>    | [ ]                                 |
| <b>Default Value:</b>    | Name supplied during installation   |
| <b>Example:</b>          | /*/imdircacheserv/dirRmeHost: [ ]   |

## dirRmeHosts

|                          |                                                                                                      |
|--------------------------|------------------------------------------------------------------------------------------------------|
| <b>Description:</b>      | Lists the hosts that are running the Directory Cache server where the RME port is available for use. |
| <b>Related Keys:</b>     | ldapServerHosts                                                                                      |
| <b>Servers Affected:</b> | Directory Cache server                                                                               |
| <b>Change Impact:</b>    | trivial                                                                                              |
| <b>Possible Values:</b>  | Any valid host name                                                                                  |
| <b>Initial Value:</b>    | [ ]                                                                                                  |
| <b>Default Value:</b>    | Names supplied during installation                                                                   |
| <b>Example:</b>          | /*/imdircacheserv/dirRmeHosts: [ ]                                                                   |

## dirRmeMaxSecondaryCalls

|                          |                                                                                        |
|--------------------------|----------------------------------------------------------------------------------------|
| <b>Description:</b>      | <i>Caution! This key should be modified only with vendor and/or technical support.</i> |
| <b>Related Keys:</b>     | none                                                                                   |
| <b>Servers Affected:</b> | Directory server, Directory Cache server                                               |
| <b>Change Impact:</b>    | trivial, no server restart required                                                    |
| <b>Possible Values:</b>  | Any integer greater than zero                                                          |
| <b>Initial Value:</b>    | 100                                                                                    |

**Default Value:** 100

**Example:** `/*/imdirserv/dirRmeMaxSecondaryCalls: [100]`

## dirRMEPort

**Description:** Is the number of the port on which the Directory server listens for RME requests.

**Related Keys:** none

**Servers Affected:** Directory server

**Change Impact:** server restart required

**Possible Values:** Any valid, unused port number

**Initial Value:** Set during installation

**Default Value:** null

**Example:** `/*/imdirserv/dirRMEPort: [5888]`

## expChgLogCommitSize

**Description:** Specifies the maximum number of changelog entries stored in the Oracle rollback segment storage area after they are deleted. When this number is reached, the deletions become permanent.

**Related Keys:** none

**Servers Affected:** Directory server

**Change Impact:** trivial

**Possible Values:** Any integer. The size of the data changed determines the value of this integer.

**Initial Value:** 1000

**Default Value:** 1000

**Example:** `/*/imdirserv/expChgLogCommitSize: [1000]`

## indexThreadSnoozePeriod

|                          |                                                                                                                               |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| <b>Description:</b>      | Specifies the number of seconds the index thread should wait before checking to see if it needs to create additional indexes. |
| <b>Related Keys:</b>     | ldapIndicesConfigRdn, initIndicesFallback                                                                                     |
| <b>Servers Affected:</b> | Directory Cache server                                                                                                        |
| <b>Change Impact:</b>    | trivial, no server restart required                                                                                           |
| <b>Possible Values:</b>  | Any number from 1 to 300                                                                                                      |
| <b>Initial Value:</b>    | 2                                                                                                                             |
| <b>Default Value:</b>    | 2                                                                                                                             |
| <b>Example:</b>          | <code>/* /common/indexThreadSnoozePeriod: [20]</code>                                                                         |

## initIndicesFallback

|                          |                                                                                                                                                                                                                                                                                                               |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description:</b>      | Specifies whether the server should read index information from the Configuration database during Directory Cache database initialization if an index entry in the Directory database is corrupted.<br>If this key is set to <code>false</code> , an error message appears and the server is not initialized. |
| <b>Related Keys:</b>     | none                                                                                                                                                                                                                                                                                                          |
| <b>Servers Affected:</b> | Directory Cache server, Directory server                                                                                                                                                                                                                                                                      |
| <b>Change Impact:</b>    | trivial                                                                                                                                                                                                                                                                                                       |
| <b>Possible Values:</b>  | true<br>false                                                                                                                                                                                                                                                                                                 |
| <b>Initial Value:</b>    | true                                                                                                                                                                                                                                                                                                          |
| <b>Default Value:</b>    | true                                                                                                                                                                                                                                                                                                          |
| <b>Example:</b>          | <code>/* /imdirserv/initIndicesFallback: [true]</code>                                                                                                                                                                                                                                                        |

## IdapAccessList

|                          |                                                                                                                      |
|--------------------------|----------------------------------------------------------------------------------------------------------------------|
| <b>Description:</b>      | Lists the IP addresses allowed to connect to the LDAP server. A value of 0.0.0.0 means all IP addresses are allowed. |
| <b>Related Keys:</b>     | anonBindAccess, defaultBindAccess, defaultBindDN, defaultBindPassword, ldapAnonymousBind, rootBindAccess             |
| <b>Servers Affected:</b> | Directory Cache server, Directory server                                                                             |
| <b>Change Impact:</b>    | trivial                                                                                                              |
| <b>Possible Values:</b>  | Any valid IP address, or netmask                                                                                     |
| <b>Initial Value:</b>    | [ ]                                                                                                                  |
| <b>Default Value:</b>    | 0.0.0.0                                                                                                              |
| <b>Example:</b>          | <code>/*/imdirserv/ldapAccessList: [0.0.0.0]</code>                                                                  |

## IdapACICacheMaxCount

|                          |                                                                     |
|--------------------------|---------------------------------------------------------------------|
| <b>Description:</b>      | Specifies the size limit of the ACI rules stored in ACIGlobalCache. |
| <b>Related Keys:</b>     | none                                                                |
| <b>Servers Affected:</b> | Directory server, Directory Cache server                            |
| <b>Change Impact:</b>    | trivial, no server restart required                                 |
| <b>Possible Values:</b>  | Any integer value greater than 0                                    |
| <b>Initial Value:</b>    | 500                                                                 |
| <b>Default Value:</b>    | 500                                                                 |
| <b>Example:</b>          | <code>/*/imdircacheserv/ldapACICacheMaxCount: [500]</code>          |

## IdapACICacheMaxSizeKB

|                      |                                                                                    |
|----------------------|------------------------------------------------------------------------------------|
| <b>Description:</b>  | Specifies the size limit, in kilobytes, of the ACI rules stored in ACIGlobalCache. |
| <b>Related Keys:</b> | none                                                                               |

|                          |                                                               |
|--------------------------|---------------------------------------------------------------|
| <b>Servers Affected:</b> | Directory server, Directory Cache server                      |
| <b>Change Impact:</b>    | trivial, no server restart required                           |
| <b>Possible Values:</b>  | Any integer value greater than 0                              |
| <b>Initial Value:</b>    | 1000                                                          |
| <b>Default Value:</b>    | 1000                                                          |
| <b>Example:</b>          | <code>/*/imdircachesserv/ldapACIcacheMaxSizeKB: [1000]</code> |

## ldapAllocRootOverride

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description:</b>      | Determines whether allocation maximums can be overridden by a user logged in as the root distinguished name (DN).<br>If this key is set to <code>true</code> , the operation is allowed if the user is logged on as the root DN and there is a directory operation that would exceed the maximum allocation for some counted attributes.<br>If this key is set to <code>false</code> , the operation is denied if the user is not logged on as the root DN and there is a directory operation that would exceed the maximum allocation for some counted attributes. |
| <b>Related Keys:</b>     | <code>ldapRootDN</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Servers Affected:</b> | Directory server                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Change Impact:</b>    | trivial, no server restart required                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Possible Values:</b>  | <code>true</code><br><code>false</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Initial Value:</b>    | <code>false</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Default Value:</b>    | <code>false</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Example:</b>          | <code>/*/imdirserv/ldapAllocRootOverride: [false]</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

## ldapAllocRuleDN

|                          |                                                                                                                 |
|--------------------------|-----------------------------------------------------------------------------------------------------------------|
| <b>Description:</b>      | Specifies the distinguished name for the entry containing the allocation rules for the InterMail administrator. |
| <b>Related Keys:</b>     | <code>none</code>                                                                                               |
| <b>Servers Affected:</b> | Directory server                                                                                                |

|                         |                                                            |
|-------------------------|------------------------------------------------------------|
| <b>Change Impact:</b>   | server restart required                                    |
| <b>Possible Values:</b> | Any distinguished name                                     |
| <b>Initial Value:</b>   | none                                                       |
| <b>Default Value:</b>   | cn=admin root                                              |
| <b>Example:</b>         | <code>/*/imdirserv/ldapAllocRuleDN: [cn=admin root]</code> |

## IdapAsyncOperation

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description:</b>      | <p>Enables/disables full asynchronous operation. In full asynchronous operation, a single LDAP connection can perform multiple operations at the same time. Each operation is executed in a separate thread, allowing operations to overlap.</p> <p>If this key is set to <code>true</code>, each operation is executed in a separate thread, allowing operations to overlap.</p> <p>If this key is set to <code>false</code>, operations other than searches are performed one at a time on each connection.</p> <p><i>Note: If asynchronous operations are used, you must ensure that entry dependency constraints are met. For example, a parent entry must be created before you can begin an operation that creates a child entry.</i></p> |
| <b>Related Keys:</b>     | <code>ldapAsyncSearch</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Servers Affected:</b> | Directory Cache server, Directory server                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Change Impact:</b>    | trivial, no server restart required                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Possible Values:</b>  | <code>true</code><br><code>false</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Initial Value:</b>    | <code>false</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Default Value:</b>    | <code>false</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Example:</b>          | <code>/*/imdirserv/ldapAsyncOperation: [false]</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

## ldapAsyncSearch

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description:</b>      | <p>Enables/disables asynchronous search operations. In asynchronous mode, a single LDAP connection can perform multiple searches simultaneously. Each search request is executed in a separate thread, allowing the searches to overlap.</p> <p>If this key is set to <code>true</code>, each search request is executed in a separate thread, allowing the searches to overlap.</p> <p>If this key is set to <code>false</code>, each search is performed one at a time, in order. All other operations are deferred until the search is complete.</p> |
| <b>Related Keys:</b>     | <code>ldapAsyncOperation</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Servers Affected:</b> | Directory Cache server, Directory server                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Change Impact:</b>    | trivial, no server restart required                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Possible Values:</b>  | <code>true</code><br><code>false</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Initial Value:</b>    | <code>false</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Default Value:</b>    | <code>false</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Example:</b>          | <code>/*/imdirserv/ldapAsyncSearch: [false]</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

## ldapBackend

|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description:</b>  | <p><b>Caution!</b> Do not change the value of this key without first consulting your InterMail vendor.</p> <p>Specifies the backend databases run by the server. These can be the Oracle database (<code>ora</code>) and/or the Oracle change logs (<code>orachglog</code>). The syntax is:</p> <pre>&lt;backendtype backendsuffix&gt;</pre> <p>Where <code>backendsuffix</code> is the highest entry of the Directory Information Tree (DIT) stored by the Directory Cache server. If no suffix is listed, the DIT root ("") is used.</p> <p><b>Note:</b> If the directory is split up among multiple backends, the portions of the DIT in the listed backends should not overlap. The code chooses the backend databases in the order listed. If there is overlap in the portions of the DIT that the backends hold, and you list a more generic suffix first, the other backends will never be called.</p> |
| <b>Related Keys:</b> | <code>changelog</code> , <code>ldapConfigDN</code> , <code>ldapSchemaDN</code> ,<br><code>ldapSchemaFile</code> , <code>writeChangeLog</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

|                          |                                                                        |
|--------------------------|------------------------------------------------------------------------|
| <b>Servers Affected:</b> | Directory Cache server, Directory server                               |
| <b>Change Impact:</b>    | server restart required                                                |
| <b>Possible Values:</b>  | ldbm<br>ora ""<br>orachglog cn=changelog                               |
| <b>Initial Value:</b>    | imdirserv: [orachglog cn=changelog]<br>[ora]<br>imdircacheserv: [ldbm] |
| <b>Default Value:</b>    | ldbm                                                                   |
| <b>Example:</b>          | /*/imdircacheserv/ldapBackend: [ldbm]                                  |

## ldapBatchTimeoutMS

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description:</b>      | <p>Specifies the timeout period, in milliseconds, that a server in batch mode will wait before doing an automatic commit of the requests it has received.</p> <p>For example, if a client sends out streams of requests to the server in a batch mode connection, the server always finds requests available on the input socket to be processed without having to wait for more requests from the client. If the request flow stops, because the client is slow or is not sending requests continuously, the server waits for the number of milliseconds specified by ldapBatchTimeoutMS before committing the requests it has received.</p> <p>This configuration key is used for batch mode as a safeguard against interrupted streams of requests.</p> |
| <b>Related Keys:</b>     | ldapMaxBatchOperations                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Servers Affected:</b> | Directory server, Directory Cache server                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Change Impact:</b>    | trivial, no server restart required                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Possible Values:</b>  | Between 1 and 86400                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Initial Value:</b>    | 20                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Default Value:</b>    | 20                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Example:</b>          | /*/common/ldapBatchTimeoutMS: [20]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

## IdapBindThruEnable

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description:</b>      | <p>Enables/disables the binding of a Directory Cache server to the master when the bind distinguished name (DN) object is not found locally.</p> <p>If this key is set to <code>true</code>, the client can bind to a directory cache where its bind DN may not exist and still perform authenticated LDAP operations, assuming proper ACLs, on any target object that exists in the bound directory cache.</p> <p>If this key is set to <code>false</code>, an LDAP client can bind to a directory cache only when the bind DN exists in the directory cache.</p> <p><i>Note: This configuration key should be set to <code>true</code> when directory caches are used together with the referral mechanism.</i></p> |
| <b>Related Keys:</b>     | none                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Servers Affected:</b> | Directory Cache server                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Change Impact:</b>    | trivial, no server restart required                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Possible Values:</b>  | <code>true</code><br><code>false</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Initial Value:</b>    | <code>false</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Default Value:</b>    | <code>false</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Example:</b>          | <code>/*/imdircachesserv/ldapBindThruEnable: [false]</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

## IdapClientTimeout

|                          |                                                        |
|--------------------------|--------------------------------------------------------|
| <b>Description:</b>      | Specifies the idle client connection timeout value.    |
| <b>Related Keys:</b>     | none                                                   |
| <b>Servers Affected:</b> | Directory Cache server, Directory server               |
| <b>Change Impact:</b>    | trivial                                                |
| <b>Possible Values:</b>  | Any numeric value, in seconds                          |
| <b>Initial Value:</b>    | 0                                                      |
| <b>Default Value:</b>    | 86400                                                  |
| <b>Example:</b>          | <code>/*/imdircachesserv/ldapClientTimeout: [0]</code> |

## IdapConfigDn

|                          |                                                                                                                                                                         |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description:</b>      | Specifies the distinguished name of the configuration node in the LDAP directory.<br><i>Caution! Do not change this value without consulting your InterMail vendor.</i> |
| <b>Related Keys:</b>     | none                                                                                                                                                                    |
| <b>Servers Affected:</b> | Directory Cache server, Directory server                                                                                                                                |
| <b>Change Impact:</b>    | server restart required                                                                                                                                                 |
| <b>Possible Values:</b>  | Any distinguished name                                                                                                                                                  |
| <b>Initial Value:</b>    | cn=config                                                                                                                                                               |
| <b>Default Value:</b>    | cn=config                                                                                                                                                               |
| <b>Example:</b>          | <code>/*/common/ldapConfigDn: [cn=config]</code>                                                                                                                        |

## IdapCosCacheMaxCount

|                          |                                                                             |
|--------------------------|-----------------------------------------------------------------------------|
| <b>Description:</b>      | Defines the maximum number of COS constraint sets kept in the memory cache. |
| <b>Related Keys:</b>     | ldapCosCacheMaxSizeKb                                                       |
| <b>Servers Affected:</b> | Directory server                                                            |
| <b>Change Impact:</b>    | trivial                                                                     |
| <b>Possible Values:</b>  | Any non-negative integer, including 0                                       |
| <b>Initial Value:</b>    | 100                                                                         |
| <b>Default Value:</b>    | 100                                                                         |
| <b>Example:</b>          | <code>/*/imdirserv/ldapCosCacheMaxCount: [100]</code>                       |

## IdapCosCacheMaxSizeKb

|                      |                                                                               |
|----------------------|-------------------------------------------------------------------------------|
| <b>Description:</b>  | Specifies the maximum size, in kilobytes, of the COS constraint memory cache. |
| <b>Related Keys:</b> | ldapCosCacheMaxCount                                                          |

**Servers Affected:** Directory server

**Change Impact:** trivial

**Possible Values:** Any non-negative integer, including 0

**Initial Value:** 0

**Default Value:** 0

**Example:** `/*/imdirserv/ldapCosCacheMaxSizeKb: [0]`

## ldapDbEntryCacheSizeInKB

**Description:** Defines the size, in kilobytes, of the database cache for LDAP entries.

**Related Keys:** `ldapDbEntryPageSizeInKB`, `ldapDbIndexCacheSizeInKB`, `ldapDbIndexPageSizeInKB`

**Servers Affected:** Directory Cache server

**Change Impact:** server restart required

**Possible Values:** Limited by system memory

**Initial Value:** 16384

**Default Value:** 16384

**Example:** `/*/imdircacheserv/ldapDBEntryCacheSizeInKB: [16384]`

## ldapDbEntryPageSizeInKB

**Description:** Specifies the database page size, in kilobytes, for LDAP entries in the Directory Cache server.

**Related Keys:** `ldapDbEntryCacheSizeInKB`, `ldapDbIndexCacheSizeInKB`, `ldapDbIndexPageSizeInKB`

**Servers Affected:** Directory Cache server

**Change Impact:** server restart required

**Possible Values:** Multiples of 8 between 8 and 64. It is recommended that you use the default value.

**Initial Value:** 16  
**Default Value:** 16  
**Example:** `/*/imdircachesserv/ldapDbEntryPageSizeInKB: [16]`

## ldapDbIndexCacheSizeInKB

**Description:** Defines the size, in kilobytes, of the database cache for LDAP indices.

**Related Keys:** `ldapDbEntryCacheSizeInKB`, `ldapDbEntryPageSizeInKB`, `ldapDbIndexPageSizeInKB`

**Servers Affected:** Directory Cache server

**Change Impact:** server restart required

**Possible Values:** Limited by system memory

**Initial Value:** 16384

**Default Value:** 16384

**Example:** `/*/imdircachesserv/ldapDbIndexCacheSizeInKB: [16384]`

## ldapDbIndexPageSizeInKB

**Description:** Specifies the page size, in kilobytes, for the LDAP index database.

**Related Keys:** `ldapDbEntryCacheSizeInKB`, `ldapDbEntryPageSizeInKB`, `ldapDbIndexCacheSizeInKB`

**Servers Affected:** Directory Cache server

**Change Impact:** server restart required

**Possible Values:** Multiples of 8 between 8 and 64

**Initial Value:** 16

**Default Value:** 16

**Example:** `/*/imdircachesserv/ldapDbIndexPageSizeInKB: [16]`

## IdapDebugWriteEnable

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description:</b>      | <p>Enables/disables the Directory Cache server debug mode. In this mode, data is written directly to the cache, with no write-through to the master.</p> <p>If this key is set to <code>true</code>, the system ignores the value of the configuration key <code>cacheDisableWriteThrus</code>, writes data to the cache, and disables write-throughs to the master.</p> <p>If this key is set to <code>false</code>, the system uses the value of the configuration key <code>cacheDisableWriteThrus</code> to determine how to write data. If the value of <code>cacheDisableWriteThrus</code> is <code>true</code>, write-throughs to the master and writes to the cache are performed. If the value of <code>cacheDisableWriteThrus</code> is <code>false</code>, writes to the cache are disabled.</p> <p><i>Note: If the value of this key is <code>true</code>, write operations are made directly to the cache with no partitioning. That is, no replication agreement data is used to determine which, if any, portion of the write is applied to the local cache. The cache is assumed to be a full replica.</i></p> |
| <b>Related Keys:</b>     | <code>cacheDisableWriteThrus</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Servers Affected:</b> | Directory Cache server                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Change Impact:</b>    | trivial, no server restart required                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Possible Values:</b>  | <code>true</code><br><code>false</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Initial Value:</b>    | <code>false</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Default Value:</b>    | <code>false</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Example:</b>          | <code>/*/imdircacheserv/ldapDebugWriteEnable: [true]</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

## IdapEnableAutoAdminGroup

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description:</b>      | <p>Specifies whether the system tries automatically to determine if the user attempting to bind to a server belongs to an InterManager administration group. If so, it enables the corresponding InterManager group privileges.</p> <p>If this key is set to <code>true</code>, an LDAP server attempts to recognize InterManager administration users binding to it. Use this setting to identify administration users from LDAP clients that are not provided with InterManager and that do not have the ability to specify InterManager administration groups explicitly.</p> <p>If this key is set to <code>false</code>, an LDAP server expects an LDAP client to specify explicitly that the user binding to the server is a member of an InterManager administration group and, therefore, wants the corresponding InterManager privileges enabled.</p> |
| <b>Related Keys:</b>     | none                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Servers Affected:</b> | Directory Cache server, Directory server                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Change Impact:</b>    | trivial, no server restart required                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Possible Values:</b>  | <code>true</code><br><code>false</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Initial Value:</b>    | <code>false</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Default Value:</b>    | <code>false</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Example:</b>          | <code>/*/imdirserv/ldapEnableAutoAdminGroup: [false]</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

## IdapEntryCacheMaxCount

|                          |                                                                                                                                                         |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description:</b>      | <p>Specifies the maximum number of LDAP entries in the entry cache. (The entry cache is an in-memory cache on top of the Sleepycat database cache.)</p> |
| <b>Related Keys:</b>     | <code>ldapEntryCacheMaxSizeKb</code>                                                                                                                    |
| <b>Servers Affected:</b> | Directory Cache server, Directory server                                                                                                                |
| <b>Change Impact:</b>    | trivial                                                                                                                                                 |
| <b>Possible Values:</b>  | Any reasonable numeric value                                                                                                                            |
| <b>Initial Value:</b>    | 1000                                                                                                                                                    |

**Default Value:** 1000

**Example:** `/*/imdircachesserv/ldapEntryCacheMaxCount: [1000]`

## ldapEntryCacheMaxSizeKb

**Description:** Specifies the maximum size of LDAP entries in the entry cache.

**Related Keys:** ldapEntryCacheMaxCount

**Servers Affected:** Directory Cache server, Directory server

**Change Impact:** trivial

**Possible Values:** Any numeric value

**Initial Value:** 1000

**Default Value:** 0 (which means no size limit)

**Example:** `/*/imdirserv/ldapEntryCacheMaxSizeKb: [10000]`

## ldapIndices

**Description:** Lists LDAP attributes to be indexed for the Directory Cache server, and how they are to be indexed. You must index all instances of the attribute since there is no means of limiting the index to a particular object class.

*Note: The Directory Cache server builds the index for you. You do not have to run a utility to build the index.*

**Related Keys:** ldapDBIndexCacheSizeInKB, ldapNumIndexDbFiles

**Servers Affected:** Directory Cache server, Directory server

**Change Impact:** server restart required

**Possible Values:** Any LDAP attributes and index actions

**Initial Value:**

```
[cn eq]
[domainname eq,reverse,unique]
[domaintype eq]
[mail eq,reverse,unique]
[mailalternateaddress eq,reverse,unique]
[mailboxid eq,unique]
[maillogin eq,unique]
[mailinglist eq,reverse]
[mailinglistpolicy eq]
[mailpolicy eq]
[mp eq]
[objectclass eq]
[rewritedomain eq]
[uid eq,reverse]
```

**Default Value:**

```
[cn eq]
[domainname eq,reverse,unique]
[domaintype eq]
[mail eq,reverse,unique]
[mailalternateaddress eq,reverse,unique]
[mailboxid eq,unique]
[maillogin eq,unique]
[mailinglist eq,reverse]
[mailinglistpolicy eq]
[mailpolicy eq]
[mp eq]
[objectclass eq]
[rewritedomain eq]
[uid eq,reverse]
```

**Example:**

```
/*/imdirserv/ldapIndices:
[cn eq]
[domainname eq,reverse,unique]
[domaintype eq]
[mail eq,reverse,unique]
[mailalternateaddress eq,reverse,unique]
[mailboxid eq,unique]
[maillogin eq,unique]
[mailinglist eq,reverse]
[mailinglistpolicy eq]
[mailpolicy eq]
[mp eq]
[objectclass eq]
[rewritedomain eq]
[uid eq,reverse]
```

## ldapIndicesConfigRdn

|                          |                                                                                                                                                       |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description:</b>      | Specifies the relative distinguished name of the indices' storage node.                                                                               |
| <b>Related Keys:</b>     | none                                                                                                                                                  |
| <b>Servers Affected:</b> | Directory Cache server, Directory server                                                                                                              |
| <b>Change Impact:</b>    | <i>Caution!</i> Changing the value of this key requires you to rebuild the database. Therefore, you should set it initially and then never change it. |
| <b>Possible Values:</b>  | <i>Caution!</i> Do not attempt to modify the value of this key.                                                                                       |
| <b>Initial Value:</b>    | cn=indices                                                                                                                                            |
| <b>Default Value:</b>    | cn=indices                                                                                                                                            |
| <b>Example:</b>          | <code>/*/common/ldapIndicesConfigRdn: [cn=newindices]</code>                                                                                          |

## ldapMasterHosts

|                          |                                                                  |
|--------------------------|------------------------------------------------------------------|
| <b>Description:</b>      | Lists the hosts on which the master Directory server is running. |
| <b>Related Keys:</b>     | none                                                             |
| <b>Servers Affected:</b> | Directory Cache server                                           |
| <b>Change Impact:</b>    | trivial                                                          |
| <b>Possible Values:</b>  | Any valid host name                                              |
| <b>Initial Value:</b>    | [ ]                                                              |
| <b>Default Value:</b>    | [ ]                                                              |
| <b>Example:</b>          | <code>*/imdircacheserv/ldapMasterHosts: [ ]</code>               |

## ldapMaxBatchOperations

|                     |                                                                                                                                                                                                                                                                                                                                        |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description:</b> | Specifies the maximum number of operations that can be run in batch mode before an automatic commit is performed.<br><br>This configuration key is used in batch mode as a safeguard against clients that do not issue <code>flush</code> requests regularly, thereby causing server-side resource utilization to grow without bounds. |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                          |                                                        |
|--------------------------|--------------------------------------------------------|
| <b>Related Keys:</b>     | none                                                   |
| <b>Servers Affected:</b> | Directory server                                       |
| <b>Change Impact:</b>    | trivial, no server restart required                    |
| <b>Possible Values:</b>  | Any number between 1 and 1000                          |
| <b>Initial Value:</b>    | 30                                                     |
| <b>Default Value:</b>    | 30                                                     |
| <b>Example:</b>          | <code>/*/imdirserv/ldapMaxBatchOperations: [30]</code> |

## ldapNumEntryDbFiles

|                          |                                                                   |
|--------------------------|-------------------------------------------------------------------|
| <b>Description:</b>      | Specifies the number of files comprising the LDAP entry database. |
| <b>Related Keys:</b>     | ldapNumIndexDbFiles                                               |
| <b>Servers Affected:</b> | Directory Cache server                                            |
| <b>Change Impact:</b>    | server restart required                                           |
| <b>Possible Values:</b>  | Any numeric value                                                 |
| <b>Initial Value:</b>    | 8                                                                 |
| <b>Default Value:</b>    | 8                                                                 |
| <b>Example:</b>          | <code>/*/imdircacheserv/ldapNumEntryDbFiles: [8]</code>           |

## ldapNumIndexDbFiles

|                          |                                                                   |
|--------------------------|-------------------------------------------------------------------|
| <b>Description:</b>      | Specifies the number of files comprising the LDAP index database. |
| <b>Related Keys:</b>     | EntryDbFiles                                                      |
| <b>Servers Affected:</b> | Directory Cache server                                            |
| <b>Change Impact:</b>    | server restart required                                           |
| <b>Possible Values:</b>  | Any numeric value                                                 |
| <b>Initial Value:</b>    | 8                                                                 |
| <b>Default Value:</b>    | 8                                                                 |

**Example:** `/*/imdircachesserv/ldapNumIndexDbFiles: [8]`

## IdapOperationLimit

**Description:** Defines the number of allowable LDAP client operations per connection.

**Related Keys:** none

**Servers Affected:** Directory Cache server, Directory server

**Change Impact:** trivial

**Possible Values:** Any numeric value

**Initial Value:** 10

**Default Value:** 10

**Example:** `/*/imdirserv/ldapOperationLimit: [10]`

## IdapPort

**Description:** Specifies the number of the port on which the Directory server or Directory Cache server listens for LDAP requests.

**Related Keys:** none

**Servers Affected:** Directory Cache server, Directory server

**Change Impact:** server restart required

**Possible Values:** Port number supplied during installation

**Initial Value:** 389

**Default Value:** 389

**Example:** `/*/imdircachesserv/ldapPort: [389]`

## IdapReplicationAgreement

**Description:** Lists the replication agreement for a Directory Cache server.

*Note: You can have only one replication agreement per Directory Cache server.*

|                          |                                                                                                                                          |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Related Keys:</b>     | attributeSelection, ldapMasterHosts, ldapPort, ldapRootDn, ldapRootPwd, partition, replAreaSpec                                          |
| <b>Servers Affected:</b> | Directory Cache server                                                                                                                   |
| <b>Change Impact:</b>    | server restart required                                                                                                                  |
| <b>Possible Values:</b>  | Unlimited                                                                                                                                |
| <b>Initial Value:</b>    | [cn: defaultReplicationAgreement]<br>[updateInterval: 60]                                                                                |
| <b>Default Value:</b>    | null                                                                                                                                     |
| <b>Example:</b>          | <pre>/*/imdircachserv/ldapReplicationAgreement:<br/>[cn: defaultReplicationAgreement]<br/>[updateInterval: 60]<br/>[replArea: RA1]</pre> |

## ldapRootDn

|                          |                                                                                                                                                                                                                                                  |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description:</b>      | Specifies the root distinguished name for the server.<br><i>Note: Do not set this configuration key on a per-host basis. To change the key, modify only the /*/common/ldapRootDN version of the key, and then restart all Directory servers.</i> |
| <b>Related Keys:</b>     | ldapRootPwd, rootBindAccess                                                                                                                                                                                                                      |
| <b>Servers Affected:</b> | Directory Cache server, Directory server                                                                                                                                                                                                         |
| <b>Change Impact:</b>    | server restart required                                                                                                                                                                                                                          |
| <b>Possible Values:</b>  | Any valid distinguished name                                                                                                                                                                                                                     |
| <b>Initial Value:</b>    | cn=root                                                                                                                                                                                                                                          |
| <b>Default Value:</b>    | cn=root                                                                                                                                                                                                                                          |
| <b>Example:</b>          | <pre>/*/imdirserv/ldapRootDn: [cn=root]</pre>                                                                                                                                                                                                    |

## ldapRootPwd

|                     |                                                                                                                                                                                                                                                        |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description:</b> | Specifies the root password for the ldap Directory server.<br><i>Note: Do not set this configuration key on a per-host basis. To change the key, modify only the /*/common/ldapRootPwd version of the key, and then restart all Directory servers.</i> |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                          |                                                      |
|--------------------------|------------------------------------------------------|
| <b>Related Keys:</b>     | <code>ldapRootDn, rootBindAccess</code>              |
| <b>Servers Affected:</b> | Directory Cache server, Directory server             |
| <b>Change Impact:</b>    | server restart required                              |
| <b>Possible Values:</b>  | Any string value                                     |
| <b>Initial Value:</b>    | <code>secret</code>                                  |
| <b>Default Value:</b>    | <code>secret</code>                                  |
| <b>Example:</b>          | <code>/*/imdircacheserv/ldapRootPwd: [secret]</code> |

## IdapSchemaCheck

|                          |                                                                                          |
|--------------------------|------------------------------------------------------------------------------------------|
| <b>Description:</b>      | Specifies whether newly added or modified objects are validated against the LDAP schema. |
| <b>Related Keys:</b>     | <code>ldapSchemaFile</code>                                                              |
| <b>Servers Affected:</b> | Directory server                                                                         |
| <b>Change Impact:</b>    | trivial, no server restart required                                                      |
| <b>Possible Values:</b>  | <code>true</code><br><code>false</code>                                                  |
| <b>Initial Value:</b>    | <code>true</code>                                                                        |
| <b>Default Value:</b>    | <code>true</code>                                                                        |
| <b>Example:</b>          | <code>/*/imdirserv/ldapSchemaCheck: [false]</code>                                       |

## IdapSchemaDn

|                          |                                                                                                                     |
|--------------------------|---------------------------------------------------------------------------------------------------------------------|
| <b>Description:</b>      | Specifies the distinguished name of the schema entry. Once the data is provisioned, this key should not be changed. |
| <b>Related Keys:</b>     | none                                                                                                                |
| <b>Servers Affected:</b> | Directory Cache server, Directory server                                                                            |
| <b>Change Impact:</b>    | server restart required                                                                                             |
| <b>Possible Values:</b>  | Any distinguished name                                                                                              |

**Initial Value:** none  
**Default Value:** cn=schema  
**Example:** /\*/imdirserv/ldapSchemaDn: [cn=schema]

## IdapSchemaFile

**Description:** Specifies the path of the schema `config` file. Paths are either absolute or relative from `$INTERMAIL`. Schema changes must be made with care, and according to the documented guidelines.

**Related Keys:** ldapSchemaCheck

**Servers Affected:** Directory Cache server, Directory server

**Change Impact:** server restart required

**Possible Values:** Any file path

**Initial Value:** config/schema.ldif

**Default Value:** none

**Example:** /\*/imdirserv/ldapSchemaFile: [config/schema.ldif]

## IdapServerHosts

**Description:** Lists the hosts running the Directory server. The C-API uses this key.

**Related Keys:** none

**Servers Affected:** Directory Cache server

**Change Impact:** no impact on server

**Possible Values:** Any valid host names

**Initial Value:** [ ]

**Default Value:** [ ]

**Example:** /\*/imdirserv/ldapServerHosts: [ ]

## ldapSizeLimit

|                          |                                                                                                                                                  |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description:</b>      | Specifies the maximum number of entries returned from a search operation when the Directory server is being used with less than root privileges. |
| <b>Related Keys:</b>     | ldapTimeLimit                                                                                                                                    |
| <b>Servers Affected:</b> | Directory Cache server, Directory server                                                                                                         |
| <b>Change Impact:</b>    | server restart required                                                                                                                          |
| <b>Possible Values:</b>  | Any numeric value                                                                                                                                |
| <b>Initial Value:</b>    | 500                                                                                                                                              |
| <b>Default Value:</b>    | 500                                                                                                                                              |
| <b>Example:</b>          | <code>/*/imdircacheserv/ldapSizeLimit: [500]</code>                                                                                              |

## ldapTimeLimit

|                          |                                                                             |
|--------------------------|-----------------------------------------------------------------------------|
| <b>Description:</b>      | Sets a time limit, in seconds, on Directory Cache server search operations. |
| <b>Related Keys:</b>     | ldapSizeLimit                                                               |
| <b>Servers Affected:</b> | Directory Cache server, Directory server                                    |
| <b>Change Impact:</b>    | server restart required                                                     |
| <b>Possible Values:</b>  | Any numeric value                                                           |
| <b>Initial Value:</b>    | imdirserv [360]<br>imdircacheserv [3600]                                    |
| <b>Default Value:</b>    | imdirserv [360]<br>imdircacheserv [3600]                                    |
| <b>Example:</b>          | <code>/*/imdircacheserv/ldapTimeLimit: [3600]</code>                        |

## logAgeHours

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description:</b>      | <p>Specifies the number of hours that entries will be kept in the change log before being automatically deleted.</p> <p>Setting <code>logAgeHours</code> and <code>logExpireHours</code> to very high values increases disk space usage, since it causes the entries in the change log to be retained for a longer time.</p> <p>Setting <code>logAgeHours</code> and <code>logExpireHours</code> to very low values causes the change logs to expire quickly. Some of the Directory Cache servers may miss this small window and be forced out of sync, requiring you to run <code>imdirsync</code> to regenerate them.</p> <p><i>Note: Changes to the <code>logAgeHours</code> value take effect after the current <code>logExpireHours</code> time period has ended.</i></p> |
| <b>Related Keys:</b>     | <code>logExpireHours</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Servers Affected:</b> | Directory server                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Change Impact:</b>    | trivial, no server restart required                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Possible Values:</b>  | 1 to $(2^{32} - 1)$                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Initial Value:</b>    | 12                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Default Value:</b>    | 12                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Example:</b>          | <code>/*/imdirserv/logAgeHours: [12]</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

## logExpireHours

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description:</b>      | <p>Defines the number of hours the system waits before deleting change log entries that are older than the value specified in the configuration key <code>logAgeHours</code>.</p> <p>Setting <code>logExpireHours</code> and <code>logAgeHours</code> to very high values increases disk space usage, since it causes the entries in the change log to be retained for a longer time.</p> <p>Setting <code>logExpireHours</code> and <code>logAgeHours</code> to very low values causes the change logs to expire quickly. Some of the Directory Cache servers may miss this small window and be forced out of sync, requiring you to run <code>imdirsync</code> to regenerate them.</p> <p><i>Note: Changes to the <code>logExpireHours</code> value take effect after the current <code>logExpireHours</code> time period has ended.</i></p> |
| <b>Related Keys:</b>     | <code>logAgeHours</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Servers Affected:</b> | Directory server                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

|                         |                                               |
|-------------------------|-----------------------------------------------|
| <b>Change Impact:</b>   | trivial, no server restart required           |
| <b>Possible Values:</b> | 1 to (232 - 1)                                |
| <b>Initial Value:</b>   | 4                                             |
| <b>Default Value:</b>   | 4                                             |
| <b>Example:</b>         | <code>/*/imdirserv/logExpireHours: [4]</code> |

## loginAliases

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description:</b>      | <p>Specifies whether the system uses alias addresses, instead of the attribute <code>userLogin</code>, to authenticate users.</p> <p>If this key is set to <code>true</code>, users can use their SMTP alias on POP or IMAP servers, instead of their POP or IMAP user login, to authenticate themselves.</p> <p>If this key is set to <code>false</code>, the user must use the attribute <code>userLogin</code> for authentication.</p> |
| <b>Related Keys:</b>     | none                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Servers Affected:</b> | Directory Cache server                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Change Impact:</b>    | trivial, no server restart required                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Possible Values:</b>  | <code>true</code><br><code>false</code>                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Initial Value:</b>    | <code>false</code>                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Default Value:</b>    | <code>false</code>                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Example:</b>          | <code>/*/imdircacheserv/loginAliases: [false]</code>                                                                                                                                                                                                                                                                                                                                                                                      |

## loginFilter

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description:</b>      | <p>A list of <code>regex</code> substitution filters that are applied, in sequence, to every name supplied in a POP authentication query before the name is looked up in the Directory database.</p> <p>The value of the <code>loginFilter</code> configuration key can include multiple entries, but each entry must appear on a separate line, contained within its own set of square brackets.</p> <p>Entries should be in the form:</p> <pre>s/pattern/replace/opts<br/>s/pattern2/replace2/opts2 ...</pre> <p>where the “/” can be any single character not used in “pattern” or “replace”, and “opts” can be empty or a string containing “g” and/or “i” (similar to Perl).</p> <p>Values are separated by a space or punctuation.</p> <p>For example:</p> <pre>s%xxx%yyy%i, s^Apple^Oracle^gi, s/^(.*)\$/Z-\1/i</pre> <p>The pattern argument is a POSIX regular expression. The replace string can be simple text, or it can contain expressions of the form “\N”, where N is a digit. If the pattern contains at least N parenthesized groups, then the text that matched the Nth group in the input will be substituted for the corresponding “\N” in the output.</p> <p><i>Note: If the IMDIAG environment variable contains "popFilter=3" before the imdircacheserv process is started, trace output will be generated that may be useful in researching issues surrounding use of this configuration key.</i></p> |
| <b>Related Keys:</b>     | none                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Servers Affected:</b> | Directory Cache Server                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Change Impact:</b>    | server restart required                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Possible Values:</b>  | A string with multiple substitution expressions                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Initial Value:</b>    | null                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Default Value:</b>    | null                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Example:</b>          | <code>/*/imdircacheserv/loginFilter: [s%xxx%yyy%i]</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

## logNumTablesLimit

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description:</b>      | Specifies the maximum number of IM_CHGLOG_YYMMDDHHMMSS tables the Directory server maintains in the database at steady state. As the specified number of such tables increases, the following performance changes occur: <ul style="list-style-type: none"><li>• The database drops stale change log entries at a faster rate.</li><li>• The Directory Cache server fetches the change log entries at a slower rate.</li></ul> <p><i>Note:</i> The number of such tables at steady state is the lesser of:</p> <ul style="list-style-type: none"><li>• The value of this configuration key</li><li>• The value of the expressing ceiling (the value of the configuration key logAgeHours divided by the value of the configuration key logExpireHours)</li></ul> |
| <b>Related Keys:</b>     | logAgeHours, logExpireHours                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Servers Affected:</b> | Directory server                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Change Impact:</b>    | trivial, no server restart required                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Possible Values:</b>  | Any value from 2 to 100                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Initial Value:</b>    | none                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Default Value:</b>    | 20                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Example:</b>          | <code>/*/imdirserv/logNumTablesLimit: [10]</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

## masterSearchRoot

|                          |                                                                        |
|--------------------------|------------------------------------------------------------------------|
| <b>Description:</b>      | Specifies the base entry to be used for searches on the master server. |
| <b>Related Keys:</b>     | none                                                                   |
| <b>Servers Affected:</b> | Directory Cache server                                                 |
| <b>Change Impact:</b>    | trivial                                                                |
| <b>Possible Values:</b>  | Any valid distinguished name                                           |
| <b>Initial Value:</b>    | [ ]                                                                    |
| <b>Default Value:</b>    | [ ]                                                                    |

**Example:** `/*/imdircachesserv/masterSearchRoot:  
[o=software.com]`

## maxCursorsPerConn

**Description:** Defines the maximum number of database cursors that a connection can retain between LDAP operations.

**Related Keys:** `primaryDBnumConnections`

**Servers Affected:** Directory Cache server

**Change Impact:** trivial

**Possible Values:** Any integer from 1 to 255

**Initial Value:** none (not in the initial `config.db` file)

**Default Value:** 8

**Example:** `/*/imdircachesserv/maxCursorsPerConn: [8]`

## modifyEntryAudit

**Description:** Indicates whether operational attributes (`modifyTimestamp` and `modifiersName`) are to be created for audit purposes for every LDAP entry.

**Related Keys:** none

**Servers Affected:** Directory server

**Change Impact:** trivial

**Possible Values:** `true`  
`false`

**Initial Value:** none

**Default Value:** `true`

**Example:** `/*/imdirserv/modifyEntryAudit: [true]`

## numLdapConnections

|                          |                                                                                                                                                                                           |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description:</b>      | Is the number of connections maintained in the pool between the client and the Directory Cache server.<br>Impacts utilities such as imdbcontrol. For imdbcontrol, the initial value is 1. |
| <b>Related Keys:</b>     | ldapMasterHosts, ldapPartitionGroup                                                                                                                                                       |
| <b>Servers Affected:</b> | Directory server, Directory Cache server                                                                                                                                                  |
| <b>Change Impact:</b>    | server restart required                                                                                                                                                                   |
| <b>Possible Values:</b>  | Any reasonable numeric value within your system limits                                                                                                                                    |
| <b>Initial Value:</b>    | 10                                                                                                                                                                                        |
| <b>Default Value:</b>    | 10                                                                                                                                                                                        |
| <b>Example:</b>          | <code>/*/imdircachesserv/numLdapConnections: [10]</code>                                                                                                                                  |

## oracleConnectWait

|                          |                                                                                                  |
|--------------------------|--------------------------------------------------------------------------------------------------|
| <b>Description:</b>      | Defines the timeout period, in seconds, for an operation waiting to obtain an Oracle connection. |
| <b>Related Keys:</b>     | none                                                                                             |
| <b>Servers Affected:</b> | Directory server                                                                                 |
| <b>Change Impact:</b>    | server restart required                                                                          |
| <b>Possible Values:</b>  | Any integer from 0 to 65535                                                                      |
| <b>Initial Value:</b>    | 60                                                                                               |
| <b>Default Value:</b>    | 60                                                                                               |
| <b>Example:</b>          | <code>/*/imdirserv/oracleConnectWait: [60]</code>                                                |

## partition

|                     |                                                                                                                                                                                                                            |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description:</b> | Defines a partition LDAP object. This object contains the definitions of the partitions in the 'partition' attribute. imdircachesserv or imdirserv use these definitions to assign the partitionName attribute to objects. |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

**Related Keys:** attributeSelection, ldapReplicationAgreement, replAreaSpec,

**Servers Affected:** Directory Cache server, Directory server

**Change Impact:** server restart required

**Possible Values:** <partition name>::BASE:<replication area Base DN>  
FILTER:<LDAP string filter syntax>

**Initial Value:** []

**Default Value:** []

**Example:**

```
/*/common/partition:
[Name: half1 Base: o=software.com Filter: (cn<=m)]
[Name: half2 Base: o=software.com Filter: (cn>m)]
[Name: small Base: o=software.com
Filter: (userLogin<=p)]
[Name: large Base: o=software.com
Filter: (userLogin>=p)]
[Name: non-leaf Base: root
Filter:(|(objectclass=domain)(objectclass=dcobject)
(objectclass=organization)
(objectclass=organizationalUnit))]
```

## primaryDbNumConnections

**Description:** Defines the number of Oracle connections in the pool available for LDAP operations.  
*Note: For Oracle licensing purposes, the backend also uses one permanent connection for bookkeeping.*

**Related Keys:** primaryDbConnection

**Servers Affected:** Directory Cache Server

**Change Impact:** server restart required

**Possible Values:** 1 to  $(2^{32} - 1)$

**Initial Value:** 4

**Default Value:** 4

**Example:**

```
/*/imdircacheserv/primaryDbNumConnections: [15]
```

## replAreaSpec

**Description:** Defines replication area specifications by referring to partition and attribute selection definitions. The names assigned to replication area specifications are referred to in the `replArea` attribute of a replication agreement.

**Related Keys:** `attributeSelection`, `partition`,  
`ldapReplicationAgreement`

**Servers Affected:** Directory Cache server

**Change Impact:** server restart required

**Possible Values:** `<replication area spec name> :: PARTITION:  
<partition name> ATTR_SEL: <attribute group name>`

**Initial Value:**

**Default Value:**

**Example:**

```

/*/imdircachesserv/replAreaSpec:
 [smallWp :: Partition: small Attr_Sel: Wp]
 [smallWpIndex :: Partition: small Attr_Sel:
WpIndex]
 [conflictRAS :: Partition: small Attr_Sel:
conflictAS]
 [largeWp :: Partition: large Attr_Sel: Wp]
 [largeWpIndex :: Partition: large Attr_Sel:
WpIndex]
 [non-leaf :: Partition: non-leaf Attr_Sel: non-
leaf]

```

## rootBindAccess

**Description:** Determines whether you can log in and authenticate if you do not log in as `root`.

If this key is set to `All`, you can log in and authenticate.

If this key is set to `Trusted`, you can log in and authenticate if you log in from a trusted IP address.

If this key is set to `None`, you cannot log in and authenticate.

**Related Keys:** `anonBindAccess`  
`defaultBindAccess`

**Servers Affected:** Directory Cache server, Directory server

|                         |                                                 |
|-------------------------|-------------------------------------------------|
| <b>Change Impact:</b>   | trivial                                         |
| <b>Possible Values:</b> | All<br>Trusted<br>None                          |
| <b>Initial Value:</b>   | All                                             |
| <b>Default Value:</b>   | None                                            |
| <b>Example:</b>         | <code>/*/imdirserv/rootBindAccess: [All]</code> |

## updateThreadRetryPeriod

|                          |                                                                       |
|--------------------------|-----------------------------------------------------------------------|
| <b>Description:</b>      | Specifies the retry interval after a failure occurs during an update. |
| <b>Related Keys:</b>     | none                                                                  |
| <b>Servers Affected:</b> | Directory Cache server                                                |
| <b>Change Impact:</b>    | server restart required                                               |
| <b>Possible Values:</b>  | Any reasonable numeric value                                          |
| <b>Initial Value:</b>    | 120                                                                   |
| <b>Default Value:</b>    | 120                                                                   |
| <b>Example:</b>          | <code>/*/imdircachesserv/updateThreadRetryPeriod: [120]</code>        |

## writeChangeLog

|                          |                                                                                                                                                                       |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description:</b>      | Indicates whether changes to the LDAP directory are to be logged in the change log.<br><i>Note: This configuration key must be set to true to enable replication.</i> |
| <b>Related Keys:</b>     | none                                                                                                                                                                  |
| <b>Servers Affected:</b> | Directory server                                                                                                                                                      |
| <b>Change Impact:</b>    | trivial                                                                                                                                                               |
| <b>Possible Values:</b>  | true<br>false                                                                                                                                                         |
| <b>Initial Value:</b>    | true                                                                                                                                                                  |

**Default Value:** true

**Example:** `/*/imdirserv/writeChangeLog: [true]`



# 9

## ***Directory Management Utilities***

---

This chapter describes the command-line utilities used to search, query, or modify Directory data in the InterMail Integrated Services Directory (ISD), which includes the Directory database and the Directory Cache database. These utilities are:

- `imaccountreport`
- `imcacheread`
- `imdbcontrol`
- `imdirmake`
- `imdirprobe`
- `imdirsync`
- `imdirupdate`
- `imldapsh`
- `imldifexport`
- `impwdhash`
- `ldapadd`
- `ldapdelete`
- `ldapmodify`
- `ldapmodrdn`
- `ldapsearch`

This chapter lists these utilities in alphabetical order. Command line utilities that affect other InterMail components in addition to the ISD are described in the *InterMail Mx Reference Guide*.

## imaccountreport

The `imaccountreport` command allows you to create a report that summarizes the number and type of accounts created after a specified date. You can print the number of active accounts, the number of suspended accounts, and the total number of accounts of all types created after this date.

### Syntax

```
imaccountreport [-date <date>] [-detail <on|off>] [-U <user>] [-W
<passwd>] [-H <host>] [-help] [Options ...]
```

Where:

|                                     |                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-date &lt;date&gt;</code>     | Sets the date for the report. Accounts created after this date are listed.<br>The date must be in the format YYYYMMDD, where Y is the four-digit year, M is the two-digit month, and D is the two-digit day.<br>If no date is specified, the current date is used.                                                                                                                                     |
| <code>-detail &lt;on off&gt;</code> | Turns the detail reporting by account status on or off.<br>Values:<br><code>on</code> : Displays the number of accounts by status.<br><code>off</code> : Displays the total number of accounts without regard to their type. Active, suspended, deleted, maintenance, proxy, and locked accounts are all included.<br>If the <code>-detail</code> argument is not specified, no details are displayed. |
| <code>-U &lt;SMTP-addr&gt;</code>   | Is the user's e-mail address.                                                                                                                                                                                                                                                                                                                                                                          |
| <code>-W &lt;passwd&gt;</code>      | Is the user's password.                                                                                                                                                                                                                                                                                                                                                                                |
| <code>-H &lt;host&gt;</code>        | Is the name of the host for the LDAP server to connect to.                                                                                                                                                                                                                                                                                                                                             |
| <code>-help</code>                  | Displays the help file for this command.                                                                                                                                                                                                                                                                                                                                                               |
| Options                             | Is an <code>imaccountreport</code> option that you can use in the shell mode. For a description of all options, see the following table.                                                                                                                                                                                                                                                               |

You can use the following options with the `imaccountreport` command:

|                     |                                                                            |
|---------------------|----------------------------------------------------------------------------|
| <code>date</code>   | Sets the date for the report. Accounts created after this date are listed. |
| <code>detail</code> | Turns the detail reporting by account status on or off.                    |

|             |                                          |
|-------------|------------------------------------------|
| bind        | Binds (or re-binds) to the LDAP server.  |
| whoami      | Shows the current bind state.            |
| run         | Runs the report.                         |
| quit or EOF | Exits the utility.                       |
| help        | Displays the help file for this command. |

## imcacheread

The `imcacheread` command prints out information about a particular user that is stored in the local Directory Cache database. This allows a quick query on a specified user, because a lookup does not need to read through to the master Directory database.

### Syntax

```
imcacheread [-help | -c | -f] [-h <host>] [<e-mailAddress> | <LoginName> <Password>]
```

Where:

|                 |                                                                                                                                                                                   |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -help           | Displays help for this command.                                                                                                                                                   |
| -c              | Displays class-of-service information for the specified address.                                                                                                                  |
| -f              | Prints forwarding addresses associated with the specified address.<br><i>Note: The <code>imbdcontrol</code> utility's <code>ListAccountForwards</code> option also does this.</i> |
| -h <host>       | Is the name of the Message Store Server (MSS) host where the mailbox resides.                                                                                                     |
| <e-mailAddress> | Is a valid e-mail address for the user.                                                                                                                                           |
| <LoginName>     | Is the POP or IMAP login name for the user.                                                                                                                                       |
| <Password>      | Is the password of the user.                                                                                                                                                      |

If you specify either a user's e-mail address or login name and password on the command line when you invoke `imcacheread`, the utility returns information about that user and then ends.

If you specify only the host, the utility goes into standard input mode and awaits input from the keyboard or from a pipe. In standard input mode, you type either an e-mail address or a POP login name and password on each line, and information about that

user is displayed. Instead of ending, `imcacheread` waits for you to specify the next user. To end the program, you must type either `^D` or `^C`.

---

**Note:** If you specify the user by e-mail address (in which case you do not specify a POP password), the password field echoes with “\*”.

---

## imdbcontrol

The `imdbcontrol` utility allows you to modify the contents of the Directory database. To execute `imdbcontrol`, you must log in as the InterMail user on any InterMail host. You can execute the utility from any directory.

---

**Note:** The `imldapsh` utility is a more powerful tool that also incorporates the capabilities of `imdbcontrol`. For more information about using the `imldapsh` utility in place of `imdbcontrol`, see page 272.

---

The `imdbcontrol` utility allows an administrator to override class-of-service settings and options set through the InterManager interface. For example, if a class of service has a maximum of three aliases for any user, InterManager strictly enforces this limit. However, using `imdbcontrol`, the administrator can override this limit. This allows flexibility when individual accounts in a class of service require expanded privileges.

### Syntax for imdbcontrol

The syntax for using `imdbcontrol` is as follows:

```
imdbcontrol [-help] [-d] [-e] [-q] [-v] [-D bindDN] [-W bindPW]
[-H host] [-P port][-p N] [-] [-h] <option>...
```

Where:

|                        |                                                                               |
|------------------------|-------------------------------------------------------------------------------|
| <code>-help</code>     | Displays help for this command.                                               |
| <code>-d</code>        | Prints debugging information during execution.                                |
| <code>-e</code>        | Causes the program to exit when it encounters errors during batch operations. |
| <code>-q</code>        | Suppresses progress reports when the program runs in batch mode.              |
| <code>-v</code>        | Reports the success or failure of each operation in batch mode.               |
| <code>-D bindDN</code> | Is the distinguished name for the server to bind as.                          |
| <code>-W bindPW</code> | Is the password for <code>bindDN</code> .                                     |
| <code>-H host</code>   | Is the name of the host for the LDAP server to connect to.                    |

|          |                                                                                                                                                                                                                                                                                        |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -P port  | Is the port number for the LDAP server.                                                                                                                                                                                                                                                |
| -p N     | Prints progress reports every N lines in batch mode. The default number of lines is 100.                                                                                                                                                                                               |
| -        | Activates batch mode. Processes multiple lines from STDIN and executes them one by one, just as if invoking each line with a separate <code>imdbcontrol</code> command. (This increases the performance of <code>imdbcontrol</code> by a factor of about 5 in doing batch operations.) |
| -h       | Displays usage information for the specified option. For example, entering <code>imdbcontrol -h CreateAccount</code> returns usage information (such as number and type of parameters) for the <code>CreateAccount</code> option.                                                      |
| <option> | Specifies the operation to perform (see “Available <code>imdbcontrol</code> Operations” on page 239).                                                                                                                                                                                  |

A command-line option specifies the operation you want `imdbcontrol` to perform. The `imdbcontrol` options fall into the following categories :

- Domains
- E-mail accounts
- Mail delivery
- SMTP aliases
- Classes of service

The `imdbcontrol` command line options are case-insensitive. For example, you can create an account by entering any of the following:

```
imdbcontrol CreateAccount ...
imdbcontrol createaccount ...
imdbcontrol CREATEACCOUNT ...
```

In addition, you can abbreviate `imdbcontrol` command line options. For example, you can express `imdbcontrol CreateAccount` as:

```
imdbcontrol ca
```

## Available `imdbcontrol` Operations

The following options are available with `imdbcontrol`. Option abbreviations are shown in parentheses.

### ***Domain Operations***

|                                |                                  |
|--------------------------------|----------------------------------|
| <code>CreateDomain (cd)</code> | Creates a mail domain.           |
| <code>DeleteDomain (dd)</code> | Deletes an existing mail domain. |

|                                        |                                                           |
|----------------------------------------|-----------------------------------------------------------|
| <code>GetDefaultDomain (gdd)</code>    | Gets the default mail domain.                             |
| <code>ListDomains (ld)</code>          | Shows a list of domains for which InterMail accepts mail. |
| <code>SetWildcardAccount (sw)</code>   | Sets the wildcard account for a local domain.             |
| <code>UnsetWildcardAccount (uw)</code> | Disables wildcard delivery for a domain.                  |
| <code>UpdateDomain (ud)</code>         | Modifies an existing domain.                              |

### **Account Operations**

|                                       |                                                                                 |
|---------------------------------------|---------------------------------------------------------------------------------|
| <code>CreateAccount (ca)</code>       | Creates an account.                                                             |
| <code>CreateAdminAccount (caa)</code> | Creates an account under an administrative organizational unit.                 |
| <code>DeleteAccount (da)</code>       | Deletes an existing account.                                                    |
| <code>DeleteAccountCos (dac)</code>   | Deletes a class-of-service value for an account.                                |
| <code>GetAccount (ga)</code>          | Gets data for an account.                                                       |
| <code>GetAccountCos (gac)</code>      | Displays the class-of-service attributes and values associated with an account. |
| <code>GetAccountFull (gaf)</code>     | Displays a full list of all the InterMail attributes for an account.            |
| <code>GetPassword (gp)</code>         | Gets the password for an existing account.                                      |
| <code>ListAccounts (la)</code>        | Shows a list of all accounts.                                                   |
| <code>ModifyAccount (ma)</code>       | Modifies an account.                                                            |
| <code>ModifyAccountPop (map)</code>   | Modifies the login name of an account.                                          |
| <code>ModifyAccountSmtP (mas)</code>  | Modifies the username of an account.                                            |
| <code>SetAccountCos (sac)</code>      | Defines a class-of-service value for an account.                                |
| <code>SetAccountQuota (saq)</code>    | Sets mailbox quotas for an account.                                             |
| <code>SetAccountStatus (sas)</code>   | Sets the status of an account, such as Active or Locked.                        |

|                         |                                                       |
|-------------------------|-------------------------------------------------------|
| SetAutoReply (sar)      | Sets the auto-reply mode for an account.              |
| SetAutoReplyHost (sarh) | Sets the location of an account's auto-reply message. |
| SetPassword (sp)        | Sets the password for an existing account.            |
| SetProxyHosts (sph)     | Set proxy hosts for an account.                       |

### **Mail Delivery Operations**

|                           |                                                                        |
|---------------------------|------------------------------------------------------------------------|
| CreateRemoteForward (crf) | Creates a remote forwarding address for an existing InterMail account. |
| DeleteRemoteForward (drf) | Deletes an existing remote forwarding address.                         |
| DisableForwarding (df)    | Disables forwarding for an account.                                    |
| DisablePOPDelivery (dpd)  | Disables local delivery (POP and IMAP) for an account.                 |
| EnableForwarding (ef)     | Enables forwarding for an account.                                     |
| EnablePOPDelivery (epd)   | Enables local delivery (POP and IMAP) for an account.                  |
| ListAccountForwards (laf) | Shows a list of forwarding addresses associated with an account.       |

### **SMTP Alias Operations**

|                  |                                       |
|------------------|---------------------------------------|
| CreateAlias (cl) | Creates an SMTP alias for an account. |
| DeleteAlias (dl) | Deletes an existing SMTP alias.       |
| ListAliases (ll) | Shows a list of SMTP aliases.         |

### **Class of Service Operations**

|                |                                 |
|----------------|---------------------------------|
| CreateCos (cc) | Creates a new class of service. |
|----------------|---------------------------------|

|                                      |                                                             |
|--------------------------------------|-------------------------------------------------------------|
| <code>DeleteCos (dc)</code>          | Deletes an existing class of service.                       |
| <code>ListCosNames (lcn)</code>      | Shows a list of existing classes of service.                |
| <code>SetCosAttribute (sca)</code>   | Sets the value of an attribute for a class of service.      |
| <code>ShowCos (sc)</code>            | Lists the attributes associated with a class of service.    |
| <code>UnsetCosAttribute (uca)</code> | Removes an attribute and its value from a class of service. |

## Domain Operations

This section describes the domain-related `imdbcontrol` operations, such as creating and deleting local mail domains.

### CreateDomain

You can create mail domains using the `imdbcontrol CreateDomain` option (abbreviated as `cd`). By default, new domains are local mail domains, but optional parameters allow you to define the new domain as a non-authoritative (semi-local) or rewrite domain.

#### Syntax

```
imdbcontrol cd <domain> [nonauth <relayHost> | rewrite <rewriteValue>]
```

Where:

|                                   |                                                                                                                                                                          |
|-----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;domain&gt;</code>       | Is the name of the new domain.                                                                                                                                           |
| <code>&lt;relayHost&gt;</code>    | Is the host to which the system routes mail received for the non-authoritative domain. This parameter is necessary only if the new domain is a non-authoritative domain. |
| <code>&lt;rewriteValue&gt;</code> | Domain name that replaces the <code>domain</code> value when header addresses are rewritten. This parameter is necessary only if the new domain is a rewrite domain.     |

### Example

The following command creates the local mail domain `software.com`.

```
imdbcontrol cd software.com
```

The following command creates the rewrite domain `accordance.com`. When mail arrives for users in this domain, the system will rewrite the domain name as `software.com`.

```
imdbcontrol cd accordance.com rewrite software.com
```

The following command creates the non-authoritative domain `venus.software.com`. When accounts in this domain receive messages, the system routes them to the host `pluto.software.com`.

```
imdbcontrol cd venus.software.com nonauth pluto.software.com
```

---

**Note:** You cannot create accounts and alias addresses in a domain until the domain exists. Also, the `CreateDomain` command will fail if the domain you are creating already exists in the database.

---

## DeleteDomain

You can delete domains using the `imdbcontrol DeleteDomain` (abbreviated as `dd`) option.

By default, deleting a domain with this option does *not* remove the domain from the Directory database. Instead, it marks the domain as deleted. This allows you to restore the domain later with the `UpdateDomain` option.

### Syntax

```
imdbcontrol dd <domain> [force]
```

Where:

|                             |                                              |
|-----------------------------|----------------------------------------------|
| <code>&lt;domain&gt;</code> | Is the name of the domain to be deleted.     |
| <code>force</code>          | Removes the domain from the ISD permanently. |

### Example

The following example deletes the domain `software.com`:

```
imdbcontrol dd software.com
```

---

**Note:** You cannot delete a domain if any accounts or alias addresses are associated with the domain. Before attempting to delete a domain, use the `ListAccounts` and `ListAliases` options to check for the existence of accounts, aliases, and forwarding addresses in the domain.

---

## GetDefaultDomain

You can retrieve the current default domain using the `imdbcontrol GetDefaultDomain` (abbreviated as `gdd`) option. This command simply outputs the name of the default domain from the Configuration database.

### Syntax

```
imdbcontrol GetDefaultDomain
```

## ListDomains

You can get a list of mail domains for which InterMail receives e-mail using the `imdbcontrol ListDomains` (abbreviated as `ld`) option. This option generates a list of domains.

### Syntax

```
imdbcontrol ListDomains
```

### Example

This command generates output like the following:

```
Domain: software.com
Type: L
RelayHost:
RewriteDomain:
WildcardAcct: unknown@software.com

Domain: venus.software.com
Type: R
RelayHost:
RewriteDomain: software.com
WildcardAcct:

^^^ # Domains = 2
```

The above data includes the following information for a domain:

- Domain name (`Domain`).
- Type of the domain (`Type`). The value of this field can be `L` (local), `N` (non-authoritative), `R` (rewrite), or `D` (deleted).
- The relay host of a non-authoritative domain (`RelayHost`). This attribute is relevant only for non-authoritative domains.
- The rewrite value of a rewrite domain (`RewriteDomain`). This value will replace the name of the rewrite domain in recipient addresses. This attribute is relevant only for rewrite domains.
- The address of the wildcard account of the local domain (`WildcardAcct`). This attribute is relevant only for local domains.

## SetWildcardAccount

All mail domains in InterMail can have an optional wildcard account associated with them. A wildcard account is simply a normal e-mail account that receives all e-mail sent to unknown addresses within the domain.

For example, if the account `john.doe@software.com` is a wildcard account for the local mail domain `software.com`, any message sent to a non-existent address within `software.com` will go to `john.doe@software.com`.

---

**Note:** Delivery to a wildcard account occurs only when the destination address of a message does not exist as an account primary address or as an SMTP alias. If the system successfully delivers a message to a normal InterMail account, it does not deliver that same message to a wildcard account as well.

---

You can set a wildcard account for a domain using the `imdbcontrol SetWildcardAccount` (abbreviated as `sw`) option.

### Syntax

```
imdbcontrol SetWildcardAccount <domain> <username>
```

Where:

|                               |                                                                                              |
|-------------------------------|----------------------------------------------------------------------------------------------|
| <code>&lt;domain&gt;</code>   | Is the name of the domain.                                                                   |
| <code>&lt;username&gt;</code> | Is the SMTP address of the e-mail account that will be the wildcard account for this domain. |

### Example

The following command sets the e-mail account `unknown@mars.software.com` as the wildcard account for the domain `mars.software.com`:

```
imdbcontrol sw mars.software.com unknown
```

## UnsetWildcardAccount

If there is a wildcard account defined for a domain, you can disable wildcard delivery by using the `imdbcontrol UnsetWildcardAccount` (abbreviated as `uw`) option.

### Syntax

```
imdbcontrol uw <domain>
```

Where:

|                             |                                                                            |
|-----------------------------|----------------------------------------------------------------------------|
| <code>&lt;domain&gt;</code> | Is the name of the domain from which you want to remove wildcard delivery. |
|-----------------------------|----------------------------------------------------------------------------|

### Example

The following command removes the wildcard account delivery defined for the domain `mars.software.com`:

```
imdbcontrol uw mars.software.com
```

---

**Note:** The `imdbcontrol UnsetWildcardAccount` command does not delete the mailbox associated with the wildcard account. In order to delete the mailbox, use the `imboxdelete` command, described in the *InterMail Mx Reference Guide*.

---

## UpdateDomain

Each domain has an associated type: `local`, `non-authoritative`, or `rewrite`. You can modify the type of an existing domain with `imdbcontrol` by using the `UpdateDomain` option.

You cannot change a `local` or `non-authoritative` domain to a `rewrite` domain directly. To make this change, set the type of a `local` or `non-authoritative` domain to `deleted`, and then set the type to `rewrite`.

### Syntax

```
imdbcontrol UpdateDomain <domain> { local | nonauth <relayHost> |
rewrite <rewriteValue> }
```

Where:

|                                   |                                                                                                                                                                         |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;domain&gt;</code>       | Name of the existing domain.                                                                                                                                            |
| <code>&lt;relayHost&gt;</code>    | Host to which the system routes mail received for the non-authoritative domain. This is necessary only if you are changing the type of the domain to non-authoritative. |
| <code>&lt;rewriteValue&gt;</code> | The domain name that replaces the domain value when rewriting header addresses. This is necessary only if you are changing the type of the domain to rewrite.           |

### Example

```
imdbcontrol UpdateDomain accordance.com nonauth mail.accordance.com
```

This command changes the domain `accordance.com` to a non-authoritative domain, and sets its relay host value to `mail.accordance.com`.

```
imdbcontrol UpdateDomain accordance.com local
```

This command changes the `accordance.com` domain to a local mail domain.

---

**Note:** You cannot create accounts and alias addresses in a rewrite domain. If you attempt to change the type of a local or non-authoritative domain to rewrite, and there are accounts associated with the domain, the operation will fail.

---

## Account Operations

The `imdbcontrol` operations described in this section are specific to InterMail account-related mail objects.

### CreateAccount

You can create accounts with `imdbcontrol` by using the `CreateAccount` option. If you omit any of the optional parameters, then you must omit all subsequent optional parameters.

#### Syntax

```
imdbcontrol ca <pSmtPAddress> <delivery-host> <internal-id>
[<PopAddress> [<password> [-convert] (clear | md5-po | unix | sha1 |
sshal) {<Domain> [(A | L | D | M | S | P) [(S | A) [<CosName>]]]]]]
```

Where:

|                                                                                        |                                                                                                                                                                                                                                        |
|----------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;pSmtPAddress&gt;</code>                                                      | Local part of the SMTP address for the account (the part that precedes the “@” symbol in the e-mail address).                                                                                                                          |
| <code>&lt;delivery-host&gt;</code>                                                     | Name of the Message Store Server (MSS) host on which to locate the mailbox for this account.                                                                                                                                           |
| <code>&lt;internal-id&gt;</code>                                                       | A unique ID shared between the Directory database and the MSS.                                                                                                                                                                         |
| <code>&lt;PopAddress&gt;</code>                                                        | POP/IMAP/WebEdge/SelfCare login name.                                                                                                                                                                                                  |
| <code>&lt;password&gt;</code>                                                          | Password for POP/IMAP/WebEdge/SelfCare access.                                                                                                                                                                                         |
| <code>-convert</code><br><code>clear md5-po unix</code><br><code> sha1   sshal)</code> | Indicates the hashing scheme used to encrypt the password. <code>clear</code> indicates that no encryption scheme is used. Note that if the <code>-convert</code> option is missing, <code>imdbcontrol</code> does not hash passwords. |
| <code>&lt;Domain&gt;</code>                                                            | Domain to associate the account with. If you do not specify a domain, the code assumes the default domain.                                                                                                                             |
| <code>A L D M S P</code>                                                               | Status of the account. The possible values for this parameter are A (active), L (locked), D (deleted), M (maintenance), S (suspended), P (proxy). The default is A (active).                                                           |

|           |                                                                                                                                        |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------|
| S A       | Account type. The possible values for this parameter are A (administrative) and S (standard). The default is S (standard).             |
| <CosName> | Class of service associated with the account. If you do not specify a class of service, the code assumes the default class of service. |

### Example

```
imdbcontrol ca john.doe pluto.software.com 12345 jdoe rosebud clear
software.com A S Basic
```

This command creates an account that has the following attributes:

- The SMTP address `john.doe` in the domain `software.com` (that is, this account has the e-mail address `john.doe@software.com`).
- A mailbox on the host `pluto.software.com`.
- The internal ID number `12345`.
- The POP/IMAP login name `jdoe`.
- The password `rosebud`.
- An account status of active (A) and an account type of standard (S).
- The class of service `Basic`.

## CreateAdminAccount

This command is similar to `CreateAccount`. It creates an account under organizational unit = administration, rather than creating it under organizational unit = consumer. This allows you to separate account information according to its delegated administrator.

### Syntax

```
imdbcontrol caa <pSmtAddress> <delivery-host> <internal-id>
[<PopAddress> [<password> [-convert] (clear | md5-po | unix | sha1 |
ssha1) {<Domain> [(A | L | D | M | S | P) [<CosName>]]]]]]
```

where each of the options and variables has the same meaning as in `CreateAccount`, above.

## DeleteAccount

You can delete accounts with `imdbcontrol` by using the `DeleteAccount` option.

### Syntax

```
imdbcontrol DeleteAccount <username> <domain>
```

Where:

|            |                                                                                                               |
|------------|---------------------------------------------------------------------------------------------------------------|
| <username> | Local part of the SMTP address for the account (the part that precedes the “@” symbol in the e-mail address). |
| <domain>   | Domain associated with the account.                                                                           |

### Example

```
imdbcontrol DeleteAccount john.doe software.com
```

This example deletes the account that has the e-mail address john.doe@software.com.

## DeleteAccountCos

You can delete a class of service attribute from an account with `imdbcontrol` by using the `DeleteAccountCos` option.

### Syntax

```
imdbcontrol DeleteAccountCos <username> <domain> <attribute>
```

Where:

|             |                                                                                                               |
|-------------|---------------------------------------------------------------------------------------------------------------|
| <username>  | Local part of the SMTP address for the account (the part that precedes the “@” symbol in the e-mail address). |
| <domain>    | Domain associated with the account.                                                                           |
| <attribute> | Name of the attribute to delete from the account.                                                             |

### Example

```
imdbcontrol DeleteAccountCos jdoe software.com mailImapAccess
```

This example deletes the class-of-service attribute `mailImapAccess` from the account `jdoe@software.com`.

## GetAccount

In addition to setting account attributes, `imdbcontrol` allows you to view all of the attributes of a particular account.

### Syntax

```
imdbcontrol ga <username> <domain>
```

Where:

|            |                                                                                                               |
|------------|---------------------------------------------------------------------------------------------------------------|
| <username> | Local part of the SMTP address for the account (the part that precedes the “@” symbol in the e-mail address). |
|------------|---------------------------------------------------------------------------------------------------------------|

<domain> Domain associated with the account.

### Example

```
imdbcontrol GetAccount john.doe software.com
```

This example retrieves all of the mail account information for the account john.doe@software.com. The output from this command looks like the following:

```
Account Info:

 Type: S
 Status: A
 Internal-ID: 10671
 Delivery Host: pluto.software.com
 Domain Name: software.com
 PSMTF Address: john.doe
 POP Address: jdoe
 Password: rosebud
 Password Hash: C
 Forward: N
 LocalDelivery: P
 AutoReply Host: pluto.software.com
 AutoReply Mode: N
 COS Name: default

```

The preceding data includes the following information for an account:

- Account type (`Type`). The value of this field can be `S` (standard) or `A` (administrative).
- Account status (`Status`). The value of this field can be `A` (active), `L` (locked), `D` (deleted), `M` (maintenance), `S` (suspended), or `P` (proxy).
- Unique number to identify the account (`Internal-ID`).
- MSS host that stores the account's mailbox (`Delivery Host`).
- Domain of the account's primary address (`Domain Name`).
- Login password (`Password`).
- Password hashing scheme (`Password Hash`). The value of this field can be `C` (clear), `U` (UNIX), or `M` (MD5).
- Flag that indicates whether mail forwarding is enabled (`Forward`). The value of this field can be `F` (enabled) or `N` (disabled).
- Flag that indicates whether local delivery is enabled (`LocalDelivery`). The value of this field can be `P` (enabled) or `N` (disabled).
- MSS host that stores the account's auto-reply message (`AutoReply Host`).
- Flag that indicates the auto-reply mode (`AutoReply Mode`). The possible values for this field are `N` (none), `V` (vacation), `R` (reply), or `E` (echo).
- Class of service associated with the account (`COS Name`).

## GetAccountCos

You can retrieve the class of service attribute values for an account with `imdbcontrol` by using the `GetAccountCos` option. This command displays the names of all InterMail class of service attributes, their values (if any) at both the class of service and account levels, and the attribute value that currently applies to the account.

### Syntax

```
imdbcontrol gac <username> <domain>
```

Where:

<username>                    Local part of the SMTP address for the account (the part that precedes the “@” symbol in the e-mail address).

<domain>                    Domain associated with the account.

### Example

```
imdbcontrol gac jdoe 7010 software.com
```

This example retrieves class of service attribute values for the account `jdoe@software.com`.

## GetAccountFull

You can display a complete list of InterMail attributes for an account using the `imdbcontrol gaf` command.

### Syntax

```
imdbcontrol gaf <smtpAddress> <domain>
```

Where:

<smtpAddress>                SMTP address for the account.

<domain>                    Domain associated with the account. If you do not specify a domain, it assumes the default domain.

## GetPassword

You can retrieve account password values with `imdbcontrol` by using the `GetPassword` option.

### Syntax

```
imdbcontrol GetPassword <username> <domain>
```

Where:

|            |                                                                                                               |
|------------|---------------------------------------------------------------------------------------------------------------|
| <username> | Local part of the SMTP address for the account (the part that precedes the “@” symbol in the e-mail address). |
| <domain>   | Domain associated with the account.                                                                           |

### Example

```
imdbcontrol GetPassword john.doe software.com
```

This command gets the password for the account `john.doe@software.com`.

## ListAccounts

While the `GetAccount` option provides information on a particular account, the `ListAccounts` option allows you to view this information for all accounts in InterMail, or in a particular domain.

### Syntax

```
imdbcontrol ListAccounts [<domain>]
```

Where:

|          |                                                                                                                    |
|----------|--------------------------------------------------------------------------------------------------------------------|
| <domain> | Domain to query for account information. If you do not specify a domain, it retrieves information for all domains. |
|----------|--------------------------------------------------------------------------------------------------------------------|

### Example

```
imdbcontrol ListAccounts software.com
```

This example retrieves mail account information for all accounts in the domain `software.com`.

```
imdbcontrol ListAccounts
```

This example retrieves mail account information for all accounts in all domains.

The mail account information includes:

- Primary e-mail address
- Login password
- Password hashing scheme. The value of this field can be C (clear), U (UNIX), or M (MD5).
- Account type. The value of this field can be S (standard) or A (administrative).
- Account status. The value of this field can be A (active), L (locked), D (deleted), M (maintenance), S (suspended), or P (proxy).
- MSS host that stores the account’s mailbox.
- Unique number to identify the account.

- Flag that indicates whether local delivery is enabled. The value of this field can be `P` (enabled) or `N` (disabled).
- Flag that indicates whether mail forwarding is enabled. The value of this field can be `F` (enabled) or `N` (disabled).
- Flag that indicates the auto-reply mode. The possible values for this field are `N` (none), `V` (vacation), `R` (reply), or `E` (echo).
- MSS host that stores the account's auto-reply message.

---

**Note:** You cannot delete a domain if the ISD has mail accounts associated with the domain. Before attempting to delete a domain, you should first use the `ListAccounts` option to check for the existence of mail accounts in this domain, and then delete those accounts if appropriate.

---

## ModifyAccount

You can modify accounts with `imdbcontrol` by using the `ModifyAccount` option. Unlike `CreateAccount`, the `ModifyAccount` option requires specifying all account parameters.

### Syntax

```
imdbcontrol ModifyAccount <username> <mssHost> <internalId> <password>
[-convert] <clear|md5|unix> <domain> <status> <type> <cosName>
```

Where:

|                                                            |                                                                                                                                                                                                                                 |
|------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <username>                                                 | Local part of the SMTP address for the account (the part that precedes the "@" symbol in the e-mail address).                                                                                                                   |
| <mssHost>                                                  | Name of the Message Store Server (MSS) host where the mailbox for this account is located.                                                                                                                                      |
| <internalId>                                               | A unique ID for the account shared between the ISD database and the MSS.                                                                                                                                                        |
| <password><br>-convert<br>clear md5 unix<br> sha1   ssha1) | Password for POP/IMAP access. If specifying a password, also indicate the hashing scheme (or lack thereof). Note that if the <code>-convert</code> option is missing, <code>imdbcontrol</code> does not hash passwords.         |
| <domain>                                                   | Domain associated with the account. If you do not specify a domain, it assumes the default domain.                                                                                                                              |
| <status>                                                   | Status of the account. The possible values for this parameter are <code>A</code> (active), <code>L</code> (locked), <code>D</code> (deleted), <code>M</code> (maintenance), <code>S</code> (suspended), <code>P</code> (proxy). |

|           |                                                                                                              |
|-----------|--------------------------------------------------------------------------------------------------------------|
| <type>    | Account type of the account. The possible values for this parameter are A (administrative) and S (standard). |
| <cosName> | Class of service associated with the account.                                                                |

### Example

```
imdbcontrol ModifyAccount john.doe pluto.software.com 12345 rosebud
unix -convert software.com A S Basic
```

This command modifies the account created in the `CreateAccount` example. The only difference is that the hashing scheme of the user's password has changed from clear to unix.

---

**Note:** When using `ModifyAccount`, it is advisable that you first execute `GetAccount` to obtain current account information, and then use `ModifyAccount` to change the account.

You cannot modify the username or domain arguments using `ModifyAccount`. In order to modify the username or domain argument, use `imdbcontrol ModifyAccountSntp`.

---

## ModifyAccountPop

You can set the login name of an account with `imdbcontrol` by using the `ModifyAccountPop` option.

### Syntax

```
imdbcontrol ModifyAccountPop <username> <domain> <popLogin>
```

Where:

|            |                                                                                                               |
|------------|---------------------------------------------------------------------------------------------------------------|
| <username> | Local part of the SMTP address for the account (the part that precedes the "@" symbol in the e-mail address). |
| <domain>   | Domain associated with the account.                                                                           |
| <popLogin> | New POP/IMAP login name value.                                                                                |

### Example

```
imdbcontrol ModifyAccountPop john.doe software.com johndoe
```

This example changes the POP/IMAP login name of the account `john.doe@software.com` to `johndoe`.

## ModifyAccountSmtplib

You can change the primary e-mail address of an account with `imdbcontrol` by using the `ModifyAccountSmtplib` option.

### Syntax

```
imdbcontrol ModifyAccountSmtplib <username> <domain> <newUsername>
<newDomain>
```

Where:

|               |                                                                                                               |
|---------------|---------------------------------------------------------------------------------------------------------------|
| <username>    | Local part of the SMTP address for the account (the part that precedes the “@” symbol in the e-mail address). |
| <domain>      | Domain associated with the account.                                                                           |
| <newUsername> | New username value for the account.                                                                           |
| <newDomain>   | New domain for the account.                                                                                   |

### Example

```
imdbcontrol ModifyAccountSmtplib john.doe software.com jdoe
sales.software.com
```

This example changes the primary e-mail address of an account from `john.doe@software.com` to `jdoe@sales.software.com`.

## SetAccountCos

You can define the value of a class-of-service attribute for an account with `imdbcontrol` by using the `SetAccountCos` option. Syntax

```
imdbcontrol SetAccountCos <username> <domain> <attribute> <value> ...
```

Where:

|             |                                                                                                               |
|-------------|---------------------------------------------------------------------------------------------------------------|
| <username>  | Local part of the SMTP address for the account (the part that precedes the “@” symbol in the e-mail address). |
| <domain>    | Domain associated with the account.                                                                           |
| <attribute> | Name of the attribute. More than one attribute can appear in a single execution, each with its own value.     |
| <value>     | Value of the attribute.                                                                                       |

You may repeat the `attribute` and `value` parameters to allow for setting multiple attributes in a single operation.

### Example

```
imdbcontrol SetAccountCos jdoe software.com mailImapAccess 1
```

This example sets values for the class-of- service attribute `mailImapAccess` for the account `jdoe@software.com`. The value `1` indicates that the command is setting this Boolean attribute to on.

## SetAccountQuota

You can set quota values at the account level with `imdbcontrol` by using the `SetAccountQuota` option. When setting values for the maximum number of messages, maximum message size, and quota warning threshold, you must specify a keyword (`maxMsgs`, `maxMsgBytes`, and `quotaThreshold`, respectively) with the value.

### Syntax

```
imdbcontrol SetAccountQuota <username> <domain><mboxMaxBytes>
[maxMsgs=<mboxMaxMsgs>] [maxMsgBytes=<mboxMaxMsgBytes>]
[quotaThreshold=<percentage>]
```

Where:

|                   |                                                                                                               |
|-------------------|---------------------------------------------------------------------------------------------------------------|
| <username>        | Local part of the SMTP address for the account (the part that precedes the “@” symbol in the e-mail address). |
| <domain>          | Domain associated with the account.                                                                           |
| <mboxMaxBytes>    | Maximum size (in bytes) of the account’s mailbox.                                                             |
| <mboxMaxMsgs>     | Maximum number of messages allowed in the account’s mailbox.                                                  |
| <mboxMaxMsgBytes> | Largest message (in bytes) that the account can receive.                                                      |
| <percentage>      | Quota warning threshold (as a percentage of the <code>mboxMaxBytes</code> limit).                             |

### Example

```
imdbcontrol SetAccountQuota john.doe software.com 10000000
maxMsgs=2000 maxMsgBytes=3000000 quotaThreshold=90
```

This command sets values for all of the available quota options for the account `john.doe@software.com`. These values set the following behaviors for the account:

- The account’s mailbox can contain no more than 10 MB (10,000,000 bytes) of mail.
- The account’s mailbox can contain no more than 2,000 messages.
- The account will accept only messages of less than 3 MB (3,000,000 bytes) .

- When the account's mailbox reaches 90% of capacity (that is, when the mailbox contains 9 MB of mail, in this case) the system sends the user a warning message.

---

**Note:** The default value for all account quotas is 0, which specifies that there are no limits on the account.

---

## SetAccountStatus

To set the status of an account, use `imdbcontrol` with the `SetAccountStatus` option.

### Syntax

```
imdbcontrol SetAccountStatus <username> <domain> <status>
```

Where:

|            |                                                                                                                                                       |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| <username> | Local part of the SMTP address for the account (the part that precedes the "@" symbol in the e-mail address).                                         |
| <domain>   | Domain associated with the account.                                                                                                                   |
| <status>   | New status of the account. The possible values for this parameter are A (active), L (locked), D (deleted), M (maintenance), S (suspended), P (proxy). |

### Example

```
imdbcontrol SetAccountStatus john.doe software.com S
```

This example changes the status of the account `john.doe@software.com` to suspended (S).

## SetAutoReply

You can enable auto-reply for an account with `imdbcontrol` by using the `SetAutoReply` option.

### Syntax

```
imdbcontrol SetAutoReply <username> <domain> <autoReplyMode>
```

Where:

|            |                                                                                                               |
|------------|---------------------------------------------------------------------------------------------------------------|
| <username> | Local part of the SMTP address for the account (the part that precedes the "@" symbol in the e-mail address). |
| <domain>   | Domain associated with the account.                                                                           |

<autoReplyMode> Mode of auto-reply the account uses. The possible values for this parameter are N (none), V (vacation), R (reply), E (echo).

### Example

```
imdbcontrol SetAutoReply john.doe software.com V
```

This example enables an auto-reply for the account `john.doe@software.com`, using the vacation mode.

---

**Note:** The ISD does not store the auto-reply message associated with an account. Therefore, `imdbcontrol` cannot set the auto-reply message. The hosts that contain account mailboxes (that is, the hosts that run the InterMail Message Store Server) store auto-reply messages as text files. Use the `SetAutoReplyHost` option with `imdbcontrol` to set the location of an account's auto-reply message.

---

## SetAutoReplyHost

All InterMail accounts include an optional auto-reply feature. The status of this feature (enabled or disabled) and its mode of operation (vacation, reply, and echo) are in the ISD. However, the actual text of an account's auto-reply message is on the file system of a host that runs the InterMail Message Store Server (MSS). Setting up the auto-reply feature for an account therefore includes specifying the MSS host on which the account's auto-reply message is stored.

You can set the location of an auto-reply message for an account with `imdbcontrol` by using the `SetAutoReplyHost` option.

### Syntax

```
imdbcontrol SetAutoReplyHost <username> <domain> <autoReplyHost>
```

Where:

|                 |                                                                                                               |
|-----------------|---------------------------------------------------------------------------------------------------------------|
| <username>      | Local part of the SMTP address for the account (the part that precedes the "@" symbol in the e-mail address). |
| <domain>        | Domain associated with the account.                                                                           |
| <autoReplyHost> | Host name of the system storing the account's auto-reply message.                                             |

### Example

```
imdbcontrol SetAutoReplyHost john.doe software.com venus.software.com
```

This command sets the host `venus.software.com` as the location of the auto-reply message for the account `john.doe@software.com`.

---

**Note:** The name of the file that contains an account's auto-reply message is in the Message Store Server (MSS) database. To specify the auto-reply file for an account, use the `imreplyctrl` command described in the *InterMail Mx Reference Guide*.

---

## SetPassword

You can set account password values with `imdbcontrol` by using the `SetPassword` option.

### Syntax

```
imdbcontrol SetPassword <username> <domain> <password> clear|md5|UNIX
[-convert]
```

Where:

|                |                                                                                                                            |
|----------------|----------------------------------------------------------------------------------------------------------------------------|
| <username>     | Local part of the SMTP address for the account (the part that precedes the "@" symbol in the e-mail address).              |
| <domain>       | Domain associated with the account.                                                                                        |
| <password>     | New password value for the account.                                                                                        |
| clear md5 UNIX | Hashing algorithm to store the password in the database.                                                                   |
| -convert       | Optional flag that specifies that <code>imdbcontrol</code> should hash the password according to the given hashing scheme. |

### Example

```
imdbcontrol SetPassword john.doe software.com $secret clear
```

This example changes the password for the account `john.doe@software.com` to `$secret`, stored in clear text format.

## SetProxyHosts

You can set a proxy host for mail access (POP/IMAP) or mail delivery (SMTP) using `imdbcontrol` with the `SetProxyHosts` option. This option is useful when you are transitioning a legacy mail system to an InterMail system, because it prevents service interruption. Mail can be accessed or delivered to the legacy system, while InterMail system integration is performed.

### Syntax

```
imdbcontrol SetProxyHosts <username> <domain> <popHost> <smtpHost>
```

Where:

|            |                                                                                                               |
|------------|---------------------------------------------------------------------------------------------------------------|
| <username> | Local part of the SMTP address for the account (the part that precedes the “@” symbol in the e-mail address). |
| <domain>   | Domain associated with the account.                                                                           |
| <popHost>  | The POP/IMAP host from which this account will access mail.                                                   |
| <smtpHost> | The SMTP host where mail for this account will be delivered.                                                  |

## Mail Delivery Operations

This section describes the `imdbcontrol` operations for mail delivery, such as options for forwarding mail from an InterMail account.

### CreateRemoteForward

To forward mail from an InterMail account to an account in a remote mail domain, create a forwarding address with `imdbcontrol` by using the `CreateRemoteForward` option.

#### Syntax

```
imdbcontrol CreateRemoteForward <username> <domain> <forwardTo>
```

Where:

|             |                                                                                                                                                           |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <username>  | Local part of the SMTP address for the account (the part that precedes the “@” symbol in the e-mail address).                                             |
| <domain>    | Domain associated with the account’s primary SMTP address. Optional only if there is a default domain. If omitted, the system assumes the default domain. |
| <forwardTo> | The complete remote address to define as a forwarding address.                                                                                            |

#### Example

```
imdbcontrol CreateRemoteForward john.doe software.com jdoe@Wossamotta-U.edu
```

This example creates the forwarding address `jdoe@Wossamotta-U.edu` for the account `john.doe@software.com`.

---

**Note:** Even if you have created a forwarding address for an account, the system will not forward mail from this account unless you have specifically enabled forwarding delivery for the account.

---

## DeleteRemoteForward

You can delete forwarding addresses from an account with `imdbcontrol` by using the `DeleteRemoteForward` option.

### Syntax

```
imdbcontrol DeleteRemoteForward <username> <domain> <forwardTo>
```

Where:

|             |                                                                                                               |
|-------------|---------------------------------------------------------------------------------------------------------------|
| <username>  | Local part of the SMTP address for the account (the part that precedes the “@” symbol in the e-mail address). |
| <domain>    | Domain associated with the account’s primary SMTP address.                                                    |
| <forwardTo> | Complete remote forwarding address to delete.                                                                 |

### Example

```
imdbcontrol DeleteRemoteForward john.doe software.com
jdoe@Wossamotta-U.edu
```

This example deletes the remote forwarding address `jdoe@Wossamotta-U.edu` that the `CreateRemoteForward` example created for the local account `john.doe@software.com`.

---

**Note:** Deleting an account’s last forwarding address automatically enables local (POP) delivery for the account, if it was previously disabled.

---

## DisableForwarding

You can disable forwarding for an account with `imdbcontrol` by using the `DisableForwarding` option. Disabling forwarding delivery this way allows you to stop mail forwarding from an account without permanently deleting all forwarding addresses associated with the account.

---

**Note:** Executing this option automatically enables local (POP) delivery if it was previously disabled.

---

### Syntax

```
imdbcontrol DisableForwarding <username> <domain>
```

Where:

|            |                                                                                                               |
|------------|---------------------------------------------------------------------------------------------------------------|
| <username> | Local part of the SMTP address for the account (the part that precedes the “@” symbol in the e-mail address). |
|------------|---------------------------------------------------------------------------------------------------------------|

<domain> Domain associated with the account's primary SMTP address.

### Example

```
imdbcontrol DisableForwarding john.doe software.com
```

This command disables forwarding delivery for the account john.doe@software.com. Once disabled, the system will not forward messages addressed to this account, regardless of whether there are any local or remote forwarding addresses defined for this account.

## DisablePOPDelivery

You can disable local delivery for an account with `imdbcontrol` by using the `DisablePOPDelivery` option.

### Syntax

```
imdbcontrol DisablePOPDelivery <username> <domain>
```

Where:

<username> Local part of the SMTP address for the account (the part that precedes the "@" symbol in the e-mail address).

<domain> Domain associated with the account.

### Example

```
imdbcontrol DisablePOPDelivery john.doe software.com
```

This command disables local delivery for the account john.doe@software.com. When you disable local delivery for an account, messages sent to that account will no longer go to the account's mailbox.

---

**Note:** An account that does not use local delivery must use mail forwarding.

---

## EnableForwarding

To enable mail forwarding for an account, use `imdbcontrol` with the `EnableForwarding` option.

### Syntax

```
imdbcontrol EnableForwarding <username> <domain>
```

Where:

<username> Local part of the SMTP address for the account (the part that precedes the "@" symbol in the e-mail address).

<domain> Domain associated with the account's primary SMTP address.

### Example

```
imdbcontrol EnableForwarding john.doe software.com
```

This command enables forwarding delivery for the account `john.doe@software.com`. With this delivery method enabled, the system will forward all messages sent to `john.doe@software.com` to the forwarding addresses defined for this account.

## EnablePOPDelivery

The most common method of mail delivery for InterMail accounts is local delivery. This method of delivery stores all messages sent to the account in a mailbox, from which a POP3 or IMAP4 mail client can access them.

You can enable local delivery for an account with `imdbcontrol` by using the `EnablePOPDelivery` option.

### Syntax

```
imdbcontrol EnablePOPDelivery <username> <domain>
```

Where:

<username> Local part of the SMTP address for the account (the part that precedes the "@" symbol in the e-mail address).

<domain> Domain associated with the account.

### Example

```
imdbcontrol EnablePOPDelivery john.doe software.com
```

This command enables local delivery for the account `john.doe@software.com`. With this delivery method enabled, all messages sent to `john.doe@software.com` will go to the account's mailbox, from which the POP3 server or IMAP server can retrieve them.

## ListAccountForwards

To get a list of the forwarding addresses that are associated with an e-mail account, use `imdbcontrol` with the `ListAccountForwards` option.

### Syntax

```
imdbcontrol ListAccountForwards <username> <domain>
```

Where:

|            |                                                                                                               |
|------------|---------------------------------------------------------------------------------------------------------------|
| <username> | Local part of the SMTP address for the account (the part that precedes the “@” symbol in the e-mail address). |
| <domain>   | Domain associated with the account’s primary SMTP address.                                                    |

### Example

```
imdbcontrol ListAccountForwards john.doe software.com
```

This command lists the local and remote forwarding addresses associated with the account `john.doe@software.com`. Output from this command includes only the relevant forwarding addresses, one per line. For example:

```
joe.schmoe@accordance.com
jdoe@Wossamotta-U.edu
```

## SMTP Alias Operations

This section describes the SMTP alias operations, such as creating, deleting, and listing alias addresses for an account.

### CreateAlias

You can create alias addresses for an account with `imdbcontrol` by using the `CreateAlias` option. If there is no default domain set, you must also specify the domains associated with these addresses. It is common to create aliases like this to let users receive mail sent to multiple addresses.

#### Syntax

```
imdbcontrol CreateAlias <username> <aliasUsername>[<domain>]
[<aliasDomain>]
```

Where:

|                 |                                                                                                               |
|-----------------|---------------------------------------------------------------------------------------------------------------|
| <username>      | Local part of the SMTP address for the account (the part that precedes the “@” symbol in the e-mail address). |
| <aliasUsername> | Local portion of the new alias address.                                                                       |
| <domain>        | Domain associated with the account’s primary SMTP address. Optional only if there is a default domain.        |
| <aliasDomain>   | Domain to associate with the new alias address. If omitted, the system assumes the default domain.            |

**Example**

```
imdbcontrol CreateAlias john.doe sales software.com
software.com
```

This command adds the alias address `sales@software.com` to the account whose primary SMTP address is `john.doe@software.com`.

**DeleteAlias**

You can delete alias addresses with `imdbcontrol` by using the `DeleteAlias` option.

**Syntax**

```
imdbcontrol DeleteAlias <username> <domain>
```

Where:

<username>            Local portion of the alias address to delete.

<domain>             Domain of the alias address.

**Example**

```
imdbcontrol DeleteAlias sales software.com
```

This command deletes the alias address `sales@software.com` created in the `CreateAlias` example.

**ListAliases**

The `ListAliases` option queries the ISD for a list of all alias addresses in the system, or the aliases associated with a particular account. You can retrieve all alias addresses in all domains by not specifying either of these variables.

**Syntax**

```
imdbcontrol ListAliases [<username> <domain>]
```

Where:

<username>            Local part of the SMTP address for the account (the part that precedes the “@” symbol in the e-mail address).

<domain>             Domain associated with the account’s primary SMTP address.

**Example**

The following command returns a list of SMTP aliases associated with the account `john.doe@software.com`:

```
imdbcontrol ListAliases john.doe software.com
```

The following example retrieves information for all alias addresses in all domains:

```
imdbcontrol ListAliases
```

---

**Note:** You cannot delete a domain if the ISD has one or more alias addresses associated with the domain. Before attempting to delete a domain, you should first use the `ListAliases` option to check for the existence of alias addresses in this domain, and then delete those aliases if appropriate.

---

## Class of Service Operations

The `imdbcontrol` operations described in this section relate to InterMail classes of service.

### CreateCos

You can create new classes of service with `imdbcontrol` by using the `CreateCos` option.

#### Syntax

```
imdbcontrol CreateCos <classOfService>
```

Where:

`<classOfService>`      Name of the new class of service.

#### Example

```
imdbcontrol CreateCos Premium
```

This example creates a new class of service named `Premium`.

### DeleteCos

You can delete classes of service with `imdbcontrol` by using the `DeleteCos` option.

#### Syntax

```
imdbcontrol DeleteCos <classOfService>
```

Where:

`<classOfService>`      Name of the class of service to delete.

#### Example

```
imdbcontrol DeleteCos Premium++
```

This command deletes the class of service named `Premium++`.

## ListCosNames

You can display the list of existing classes of service with `imdbcontrol` by using the `ListCosNames` option.

### Syntax

```
imdbcontrol ListCosNames
```

## SetCosAttribute

You can define the value of an attribute for a class of service with `imdbcontrol` by using the `SetCosAttribute` option.

### Syntax

```
imdbcontrol SetCosAttribute <classOfService> <attribute> <value>
```

Where:

<classOfService>      Name of the class of service for which to define the attribute.

<attribute>            Name of the attribute.

<value>                Value of the attribute.

### Example

```
imdbcontrol SetCosAttribute Basic mailPopAccess all
```

This example sets the attribute `mailPopAccess` for a class of service named `Basic`. The value `all` indicates that POP access is allowed from all locations.

## ShowCos

You can display the attributes associated with a class of service, including their values, by using the `imdbcontrol ShowCos` option.

### Syntax

```
imdbcontrol ShowCos <classOfService>
```

Where:

<classOfService>      Name of the class of service to query.

### Example

```
imdbcontrol ShowCos Premium
```

This command lists the attributes associated with the class of service named Premium++. This command generates output like the following:

```
mailPopAccess:all
mailSmtAccess:1
```

## UnsetCosAttribute

You can delete an attribute from a class of service with `imdbcontrol` by using the `SetCosAttribute` option. When this option executes, it deletes the existing value of the attribute for the given class of service, which is no longer associated with that attribute.

### Syntax

```
imdbcontrol UnsetCosAttribute <classOfService> <attribute>
```

Where:

<classOfService>      Name of the class of service for which to remove the attribute.

<attribute>            Name of the attribute.

### Example

```
imdbcontrol UnsetCosAttribute Basic mailPopSslAccess
```

This example disassociates the attribute `mailPopSslAccess` from a class of service named `Basic`. This deletes the value for this attribute in the `Basic` class of service.

## imdirmake

The `imdirmake` command is used to create a new database or to destroy an existing database.

---

**Caution!** Ensure that the Directory server and Directory Cache servers are shut down before running the `imdirmake` command. Use this command only after consulting with your InterMail vendor or technical support staff.

---

### Syntax

```
imdirmake [-c|-d|-r|-h] [-q] [imdirserv|imdircachserv]
```

Where:

-c                      Creates and initializes a new database. This is the default mode.

-d                      Destroys an existing Directory Cache database.

|    |                                                                        |
|----|------------------------------------------------------------------------|
| -r | Destroys an existing Directory Cache database, then creates a new one. |
| -h | Displays Help file.                                                    |
| -q | Quiet, non-interactive mode.                                           |

To re-create the master Directory database, use the SQL scripts `resetLDAP.sql` found in the `mercury/ldap/back-ora` directory.

## imdirprobe

The `imdirprobe` command checks a set of InterMail accounts and verifies that each has a given value for the MSS host and/or account status. The `imdirprobe` command can also update the Directory Cache database and confirm the MSS host and account status for a specified set of InterMail accounts. It accomplishes this by accessing either the Directory server or the Directory Cache servers.

### Syntax

```
imdirprobe {-cache <hosts> | -master} <addresses>
[-t <threads>][-u] [-p <pass>] [-f <fail>] [-h <host>]
[-m <mode>]
```

### Where:

|              |                                                                                                                                               |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| -cache       | Tells <code>imdirprobe</code> to use the Directory Cache servers.                                                                             |
| <hosts>      | Is a colon-separated list of hosts running Directory Cache servers.                                                                           |
| -master      | Tells <code>imdirprobe</code> to use the master Directory server.                                                                             |
| <addresses>  | Is a file containing e-mail addresses, one per line.                                                                                          |
| -t <threads> | Specifies the number of threads to be run per cache server. The default value is 1. You cannot use this parameter with <code>-master</code> . |
| -u           | Forces a cache update (using a bad password). Not allowed with <code>-master</code> .                                                         |
| -p <pass>    | Specifies an output file for addresses that succeed (the default is <code>imdirprobe.pass</code> ).                                           |
| -f <fail>    | Specifies an output file for addresses that fail (the default is <code>imdirprobe.fail</code> ).                                              |
| -h <host>    | Specifies the MSS host for the specified addresses.                                                                                           |
| -m <mode>    | Specifies the mode (A, S, M) of the specified addresses.                                                                                      |

## imdirsync

The `imdirsync` command is a database synchronization command used to bring the Directory Cache database up to date with the master Directory database.

The `imdirsync` command retrieves the partitions of the master Directory database that the Directory Cache database is configured to store, and creates a new Directory Cache database. It then sends a message to the Directory Cache server to close its internal caches and files and open the newly created Directory Cache database.

### Syntax

```
imdirsync
```

## imdirupdate

The `imdirupdate` command is a batch command that writes the same information to multiple InterMail account entries in the master Directory database. The type of information that it can write includes the status of the account (A for Active, M for Maintenance, P for Proxy, L for Locked, or S for Suspended) and the MSS host on which the mailbox for this user resides.

### Syntax

```
imdirupdate [-h <host>] [-m <status>] <accounts>
```

Where:

- |                                |                                               |
|--------------------------------|-----------------------------------------------|
| <code>-h &lt;host&gt;</code>   | Changes the MSS host of the accounts.         |
| <code>-m &lt;status&gt;</code> | Changes the status of the accounts.           |
| <code>&lt;accounts&gt;</code>  | Is a file containing a list of account names. |

### Example

In order to change information for multiple account entries in the ISD, you must first run `imaccountquery` to find out information on the relevant InterMail accounts:

```
venus% imaccountquery -r full -or -s A -s L
....
```

Next, use `vi` or another editor to create an input file containing e-mail addresses (one per line) of each account to be updated with `imdirupdate`.

Finally, run `imdirupdate` on the file:

```
venus% imdirupdate -m A imdirupdate.in
imdirupdate: fetching account information...
imdirupdate: updating accounts...
imdbcontrol cmd done:
imdirupdate: done.
```

---

**Note:** It is recommended that, after running `imdirupdate`, you run `imaccountquery` again to confirm your account changes.

---

## imldapsh

The `imldapsh` command provides a shell-like interface that allows you to search and modify the contents of the Directory database at a deeper level than is possible with the `imdbcontrol` command. In addition, you can use `imldapsh` as a command-line tool instead of `imdbcontrol`.

Using `imldapsh`, you can go directly into the Directory Information Tree (DIT) and modify attributes for any entry with precision. Schema-checking mechanisms on the Directory server prevent accidental schema violations. Access Control Information (ACI) filters prevent unauthorized users from modifying the Directory database. The Directory schema and DIT are described in detail in Chapter 7.

`imldapsh` maintains a current working distinguished name (DN) similar to the "current working directory" in a UNIX shell. After the Directory server authenticates your user identification (either your e-mail address or the DN of your person entry) and your password, you start out with your current working DN at the top of the directory tree. Use the `ls` command to see the "children" of the current entry, which are listed as relative distinguished names (RDNs).

Using `imldapsh`, you can:

- Log in to the Directory server
- Change the current working DN
- View the attribute names and values of any entry in read-only mode
- Add, modify, or delete the attribute values of any entry
- Add, modify, or delete an entry

In addition to basic LDAP functionality, `imldapsh` also includes:

- Variable substitution
- Output redirection

The `imldapsh` utility supports variable definition and substitution in the command line. The syntax for variables is `$(variablename)`.

Commands that operate on variables are:

- `setvar` sets the variable. For example:  

```
setvar foo "dn=bar"
```
- `unsetvar` unsets the variable. For example:  

```
unsetvar foo
```
- `printvar` displays all the currently defined `imldapsh` variables

You can redirect the output of any `imldapsh` command to a file using `>`. For example, the following causes the output of the `ls` command to be written to the file `directory-listing.txt`:

```
imldapsh> ls -r > directory-listing.txt
```

### Syntax

```
imldapsh [-U <SMTP-addr>] [-D <bindDN>] [-W <passwd>] [-H <host>]
[-P <port>] [-F <scriptFile>] [-help] [-d] [-e] [-v] [option ...]
```

Where:

|                                    |                                                                                                                                  |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| <code>-U &lt;SMTP-addr&gt;</code>  | Is the user's e-mail address                                                                                                     |
| <code>-D &lt;bindDN&gt;</code>     | Is the distinguished name to bind as                                                                                             |
| <code>-W &lt;passwd&gt;</code>     | Is the password for bindDN.                                                                                                      |
| <code>-H &lt;host&gt;</code>       | Is the name of the host for the LDAP server to connect to.                                                                       |
| <code>-P &lt;port&gt;</code>       | Is the port number for the LDAP server.                                                                                          |
| <code>-F &lt;scriptFile&gt;</code> | Is the name of a batch file containing a list of <code>imldapsh</code> commands.                                                 |
| <code>-help</code>                 | Displays help for this command.                                                                                                  |
| <code>-d</code>                    | Prints debug information.                                                                                                        |
| <code>-e</code>                    | Specifies that the utility is to exit when errors are encountered in batch mode.                                                 |
| <code>-v</code>                    | Reports success or failure of each command.                                                                                      |
| <code>option</code>                | Is an <code>imldapsh</code> option. For a description of all options, see the following section, <code>imldapsh Options</code> . |

### *imldapsh Options*

The following table provides information on the commands that are available with `imldapsh`:

|                                       |                                                        |
|---------------------------------------|--------------------------------------------------------|
| <code>help</code>                     | Displays help for this command.                        |
| <code>quit</code> or <code>EOF</code> | Exits the program.                                     |
| <code>pathsep &lt;char&gt;</code>     | Changes the path separator.<br>Default: <code>/</code> |
| <code>dnsep &lt;char&gt;</code>       | Changes the DN separator.<br>Default: <code>,</code>   |

|                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>bind &lt;name&gt;<br/>&lt;passwd&gt;</p>                   | <p>Logs in and authenticates you to the Directory server. &lt;name&gt; must be root or a valid SMTP address. &lt;passwd&gt; is your user password.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <p>login &lt;name&gt;<br/>&lt;passwd&gt;</p>                  | <p>Is a synonym for bind.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <p>whoami</p>                                                 | <p>Displays the current bind state; if the server is bound, the username, host, and port number of the server are displayed.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <p>cd &lt;path&gt;</p>                                        | <p>Changes the current working DN using an absolute &lt;path&gt; or a &lt;path&gt; relative to the current DN.<br/>&lt;path&gt; is an absolute or relative path of the form<br/>[ / ] RDN or [ /RDN...]<br/>in parent-to-leaf order, meaning that the most significant components come first.<br/>The RDNs must be separated by / with no spaces.<br/>If the first character is /, &lt;path&gt; is an absolute path, starting at the top of the DIT. Otherwise, it is a path relative to the current working DN.<br/>You can also use:<br/>. to represent the RDN of the current working DN.<br/>.. to represent the RDN of an entry's parent.</p> |
| <p>dn &lt;DN&gt;</p>                                          | <p>Sets the current working DN to &lt;DN&gt;. &lt;DN&gt; must be absolute and complete. The DN is in LDAP canonical leaf to parent order.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <p>pwd</p>                                                    | <p>Displays the current working DN, so that you can see where you are in the DIT. The DN is displayed in LDAP canonical leaf to parent order.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <p>pwp</p>                                                    | <p>Displays the current working path, so that you can see the working location in the LDAP DIT as a path.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <p>ls [-r] [-l]<br/>[-c &lt;class&gt;]<br/>[&lt;path&gt;]</p> | <p>Lists the children of the current entry, that is, the RDNs of the entries beneath &lt;path&gt;.<br/>-r Performs a recursive list, showing the entire tree under the current location.<br/>-l Shows the full DN of each child displayed.<br/>-c &lt;class&gt; Shows only entries of the type &lt;class&gt;.</p>                                                                                                                                                                                                                                                                                                                                  |

|                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>show [-i -r]<br/>[&lt;path&gt;]</code>            | <p>Shows the attribute names and their values in the entry at <code>pathname &lt;path&gt;</code>.</p> <p>If you do not specify a path, the entry of the current working DN is shown.</p> <p><code>-i</code> Shows the attributes of the immediate children of the entry at <code>&lt;path&gt;</code>.</p> <p><code>-r</code> Shows the attributes of all descendents of the entry at <code>&lt;path&gt;</code>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <code>cat</code>                                        | <p>Is a synonym for <code>show</code>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <code>edit [&lt;path&gt;]</code>                        | <p>Modifies the attribute values of the entry at <code>&lt;path&gt;</code> using the text editor specified in the <code>\\$EDITOR</code> environment variable. The default text editor is <code>vi</code>.</p> <p>The <code>edit</code> command creates a temporary file in LDAP Data Interchange Format (LDIF). Each line of the LDIF file represents an attribute.</p> <p>To delete an attribute, delete the line.</p> <p>To modify an attribute, change the value after the colon ( : ) on the line.</p> <p>To add an attribute, add a new line in the form:</p> <pre>name:value</pre> <p>If your changes violate the LDAP schema, or if you do not have permission to modify the entry, your edits will not be accepted.</p> <p>If you decide to abort the edit, you should delete the entire contents of the temporary file and save it. If you do this, no modifications will be made.</p> |
| <code>view [&lt;path&gt;]</code>                        | <p>Displays the entry at <code>&lt;path&gt;</code> in read-only mode using <code>\\$EDITOR</code> (by default <code>vi</code>).</p> <p>This option works exactly like the <code>edit</code> option except that the displayed file is not used to modify the Directory database.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <code>rm [-r] [&lt;path&gt;]</code>                     | <p>Removes the entry at <code>&lt;path&gt;</code>.</p> <p><code>-r</code> recursively removes entries under <code>&lt;path&gt;</code>.</p> <p>If <code>-r</code> is used, <code>&lt;path&gt;</code> must specify a leaf node.</p> <p>If the <code>&lt;path&gt;</code> argument is absent, this command operates on the current working path.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <code>rename [-k]<br/>[&lt;path&gt;] &lt;rdn&gt;</code> | <p>Renames the entry specified in <code>&lt;path&gt;</code> to <code>&lt;rdn&gt;</code>. If the <code>-k</code> argument is specified, the old RDN is retained as a simple attribute of the specified entry.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

|                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| setattr [-m]<br>[-p <path>]<br><attributeName><br><attributeValue>   | Sets the attribute specified by <attributeName> of the entry at <path>, and gives it the value specified by <attributeValue>.<br><br>-m Specifies that the attribute has multiple values. This value does not replace a value already assigned to the attribute but is added as an additional value<br><br>-p Specifies the path of the entry to be operated on. If this argument is not specified, the current working path is used.                                                                                                                                                              |
| unsetattr [-m]<br>[-p <path>]<br><attributeName><br><attributeValue> | Unsets the attribute specified by <attributeName> of the entry at <path>. If you use the -m argument, you can specify the optional <attributeValue> argument to indicate that his value should be removed from the attribute. If the -m argument is not specified, the <attributeValue> argument is ignored and the entire attribute is removed from the entry given by the <path> argument.                                                                                                                                                                                                       |
| new [-v] <path><br>[<template>]                                      | Creates an entry under the specified <path>, using \$EDITOR.<br><template> A file containing LDIF-formatted data that is loaded into the editor to simplify creation of the new entry.<br><br>-v Causes the commands to display on standard output the entry that it is about to be created.<br><br><i>Note: The DN of the entry to be created must end in an RDN that does not already exist. Therefore, the DN cannot be specified in the current working path, which must exist in the Directory.</i><br><br>You cannot use this command in batch mode. You can use the ldapdd utility instead. |
| import [-v]<br>[-p <path>]<br><filename>                             | Reads LDIF formatted data from <filename> and creates a new entry.<br><br>-v Displays the entry to be created on the standard output.<br><br>-p Causes the DN of the new entry to be generated from <path>; if this argument is not specified, the DN attribute of the input file is used.                                                                                                                                                                                                                                                                                                         |
| export [-p <path>]<br><outputfile>                                   | Writes LDIF formatted data describing the database entry at <path> to the file specified in <outputfile>. If <path> is not specified, the current working path is used.                                                                                                                                                                                                                                                                                                                                                                                                                            |
| ! <command>                                                          | Executes <command> in a sub-shell.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

---

**Note:** If spaces are a significant part of the LDAP DNs of attribute values, you can use quotation marks to eliminate any confusion. For example,  
cd "cn=admin root".

---

All DN syntax is interpreted as absolute. You can use the path syntax in `imldapsh` to specify relative locations in the LDAP DIT. For example, the DN syntax “`cn=site,cn=admin root`” and the path syntax “`/cn=admin root/cn=site`” both specify the same location.

```
imldapsh> DN "cn=site,cn=admin root"
```

```
imldapsh> cd "/cn=admin root"
imldapsh> cd "cn=site"
```

### **Special Variables**

The `imldapsh` utility maintains the following special variables:

|                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>cwdn</code>           | Is the current working DN.                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <code>cwp</code>            | Is the current working path.                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <code>host</code>           | Is the hostname of the machine where the LDAP server is running.                                                                                                                                                                                                                                                                                                                                                                                       |
| <code>port</code>           | Is the port number used to bind to the LDAP server.                                                                                                                                                                                                                                                                                                                                                                                                    |
| <code>user</code>           | Is the name used to bind to the LDAP server.                                                                                                                                                                                                                                                                                                                                                                                                           |
| <code>imdbcAdminRoot</code> | Is a DN which tells certain <code>imdbcontrol</code> -like commands where in the DIT to look for <code>adminPolicies</code> (classes of service). For a list of the commands that use this variable, see “Using <code>imldapsh</code> Instead of <code>imdbcontrol</code> ” on page 276.<br><br>This variable is set by the user or inherits the value from the UNIX shell variable <code>IMDBCADMINROOT</code> when <code>imldapsh</code> is started. |

### **Using `imldapsh` Instead of `imdbcontrol`**

It is recommended that you use the `imldapsh` utility as a replacement for `imdbcontrol`. It accepts most of the `imdbcontrol` arguments and command syntax. The earlier version of `imdbcontrol` allowed creation of accounts and classes of service in a fixed position only; with this version you can create these objects in various locations in the DIT.

To use some of the `imdbcontrol` options, you need to input a special variable `IMDBCADMINROOT`. The value of this variable is a distinguished name within the admin subtree of the DIT where `AdminPolicies` (or classes of services) can be found and created. The `imldapsh` utility reads the value of the shell environment variable `IMDBCADMINROOT` on startup and uses this value as the initial value of its own `imdbcAdminRoot` variable. If `IMDBCADMINROOT` is not defined in the shell environment where `imldapsh` is started, the `imldapsh` utility uses “`cn=site,cn=admin root`” as the initial value.

The `imdbcontrol` options that require the setting of the `IMDBCADMINROOT` variable are:

- CreateAccount (ca)
- CreateCos (cc)
- DeleteCos (dc)
- ShowCos (sc)
- SetCosAttribute (sca)
- UnsetCosAttribute (uca)

The following imdbcontrol arguments are supported without change by imldapsh:

- |                             |                             |
|-----------------------------|-----------------------------|
| • CreateDomain              | • UpdateDomain (ud)         |
| • DeleteDomain (dd)         | • GetDefaultDomain (gdd)    |
| • ListDomains (ld)          | • SetWildcardAccount (sw)   |
| • UnsetWildcardAccount (uw) | • DeleteAccount (da)        |
| • DeleteAccount (da)        | • DeleteAccountCos (dac)    |
| • GetAccount (ga)           | • GetAccountFull (gaf)      |
| • GetPassword (gp)          | • GetAccountCos (gac)       |
| • ListAccounts (la)         | • ModifyAccount (ma)        |
| • ModifyAccountPop (map)    | • ModifyAccountSmtP (mas)   |
| • SetAccountStatus (sas)    | • SetAutoReply (sar)        |
| • SetAutoReplyHost (sarh)   | • SetPassword (sp)          |
| • SetAccountQuota (saq)     | • SetAccountCos (sac)       |
| • SetProxyHosts (sph)       | • CreateAlias (cl)          |
| • DeleteAlias (dl)          | • ListAliases (ll)          |
| • CreateRemoteForward (crf) | • DeleteRemoteForward (drf) |
| • DisableForwarding (df)    | • DisablePopDelevery (dpd)  |
| • EnableForwarding (ef)     | • EnablePopDelivery (epd)   |
| • ListAccountForwards (laf) | • ListCosNames (lcn)        |

For information on the imdbcontrol arguments, see “imdbcontrol” on page 238.

### Example 1

To create an account from a UNIX shell, first set the UNIX shell environment variable IMDBCADMINROOT. Enter:

```
setenv IMDBCADMINROOT "cn=site,cn=admin root"
```

Once the variable is set, enter:

```
imldapsh ca john.doe pluto.software.com 12345 jdoe rosebud clear
software.com A S Basic
```

This command creates an account that has the following attributes:

- The SMTP address `john.doe` in the domain `software.com` (that is, this account has the e-mail address `john.doe@software.com`).
- A mailbox on the host `pluto.software.com`.
- The internal ID number `12345`.
- The POP/IMAP login name `jdoe`.
- The password `rosebud`.
- An account status of active (A) and an account type of standard (S).
- The class of service `Basic`.

You can also create the same account using `imldapsh` in the shell mode. A transcript of such a session may look like the following:

```
% imldapsh
imldapsh: LDAP server at hostname:17705 (not bound)
imldapsh (not bound)> bind root secret
imldapsh: binding as root at hostname:17705
imldapsh> setvar IMDBCADMINROOT "cn=site,cn=admin root"
imldapsh> ca john.doe pluto.software.com 12345 jdoe rosebud
clear software.com A S Basic
```

## Example 2

To delete an account, enter:

```
imldapsh -D cn=root -W secret da john.doe software.com
```

This example deletes the account that has the e-mail address `john.doe@software.com`.

You can also delete the account using `imldapsh` in the shell mode. A transcript of such a session may look like the following:

```
% imldapsh
imldapsh: LDAP server at hostname:17705 (not bound)
imldapsh (not bound)> bind root secret
imldapsh: binding as root at hostname:17705
imldapsh> da john.doe software.com
imldapsh> exit
```

## imldifexport

The `imldifexport` command allows you to export data from the InterMail master Directory database or from a Directory Cache database to a foreign LDAP directory. It causes all of the data in the database, except the Oracle changelog data, to be printed

to standard output in LDAP Data Interchange Format (LDIF). Changelog data is not exported. LDIF is a standard way of representing directory data in a text file format, used to export and import data among LDAP directories. It consists of a series of lines of ASCII text, beginning with the distinguished name of a directory entry, and listing the attributes of the entry, with one attribute on each line.

The Directory server and the Directory Cache server should not be running when you issue this command.

### Syntax

```
imldifexport [imdircachserv|imdirserv]
```

Where:

|                            |                                                                                                    |
|----------------------------|----------------------------------------------------------------------------------------------------|
| <code>imdircachserv</code> | Is the process name for the Directory Cache server. This is the default if no option is specified. |
| <code>imdirserv</code>     | Is the process name for the Directory server.                                                      |

## impwdhash

The `impwdhash` command allows the user to store passwords in a hashed format. The `impwdhash` command takes clear-text strings as input and scrambles them, resulting in an apparently random binary string (called a “hash”) from which you cannot recover the original plain text. There is no way to determine what this hashed password is by looking at either the Directory Cache database or the master Directory database, because, unlike encryption, hashing is a one-way algorithm. The only way to return the clear-text equivalent value of a hash is to take another clear-text value, run it through the same hashing algorithm, and compare the result. If you have a match, you know that the new plain text matches the original plain text.

The system supports two forms of hashing: MD5-PO and UNIX [`crypt()` algorithm]. InterMail supports the capability to specify different hash schemes on a per-user basis. The ISD stores user passwords as well as hashed passwords.

---

**Note:** Typically, you use the `impwdhash` command in conjunction with `imdbcontrol` to get and set hashed passwords.

---

### Syntax

```
impwdhash -a [md5-po|unix] <Password> [<hashedPassword>]
```

Where:

|                     |                                        |
|---------------------|----------------------------------------|
| <code>-a</code>     | Algorithm strategy to use for hashing. |
| <code>md5-po</code> | MD5-PO hashing strategy                |

|                  |                               |
|------------------|-------------------------------|
| unix             | UNIX hashing strategy         |
| <Password>       | POP password for the account. |
| <hashedPassword> | Hashed password.              |

### Example

To set a password, run `impwdhash` in conjunction with `imdbcontrol`, as in the following example:

---

**Note:** The following example includes the creation of a new user account. For more information on account creation, see the *InterMail Mx Operations Guide*.

---

```
paris% impwdhash -a unix secret f3HiwyRyBcEX2
paris% imldapsh
imldapsh: LDAP server at hostname:17705 (not bound)
imldapsh (not bound)> bind root secret
imldapsh: binding as root at hostname:17705
imldapsh> setvar IMDBCADMINROOT "cn=site,cn=admin root"
imldapsh> ca john.doe paris@software.com 25 jdoe f3HiwyRyBcEX2 unix
software.com A S Basic
```

In this example, we first have hashed the password “secret.” Then the hashed password and password algorithm are input into `imldapsh` as it creates the account. Now, although the hashed string “f3HiwyRyBcEX2” is in the ISD, you still see the “secret” password when identifying yourself to the POP server.

## ldapadd

The `ldapadd` command allows you to add new entries to the Directory database. `ldapadd` is a special instance of `ldapmodify`.

---

**Note:** If you want to add entries and also perform other operations in the same file, use the `ldapmodify` command for all of the operations.

---

The `ldapadd` command supports UTF-8 input.

### Syntax

```
ldapadd [-b] [-c] [-r] [-n] [-v] [-d <level>] [-D <binddn>]
[-w <passwd>][-h <host>] [-p <port>] [-f <file>] [-g <adminGroupDN>]
[-m]
```

## Where:

|                   |                                                                                                                                                                                                                                                                                                                 |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -b                | Assumes that any values that start with a <code>'</code> are binary values, and that the actual value is in a file whose path is specified in the place where values normally appear.                                                                                                                           |
| -c                | Continuous operation mode. Errors are reported, but <code>ldapadd</code> will continue to operate with modifications. The default is to exit after reporting an error.                                                                                                                                          |
| -r                | Replaces existing values by default.                                                                                                                                                                                                                                                                            |
| -n                | Shows what would be done, but doesn't actually add entries. Useful for debugging in conjunction with <code>-v</code> .                                                                                                                                                                                          |
| -v                | Uses verbose mode, with many diagnostics written to standard output.                                                                                                                                                                                                                                            |
| -d <level>        | Sets the LDAP debugging level to <level>.                                                                                                                                                                                                                                                                       |
| -D <binddn>       | Uses <binddn> to bind to the directory. <binddn> should be a string-represented distinguished name as defined in RFC 1779.                                                                                                                                                                                      |
| -w <passwd>       | Uses <password> as the password for simple authentication.                                                                                                                                                                                                                                                      |
| -h <host>         | Specifies an alternate host on which the LDAP server is running.                                                                                                                                                                                                                                                |
| -p <port>         | Specifies an alternate TCP port where the LDAP server is listening.                                                                                                                                                                                                                                             |
| -f <file>         | Reads the entry modification information from the LDIF file <file> instead of from standard input.                                                                                                                                                                                                              |
| -g <adminGroupDN> | Specifies the DN for the InterManager adminGroup that the user wants to bind as to get elevated permissions.                                                                                                                                                                                                    |
| -m                | Enables batch mode. When this option is specified, all operations that this utility normally performs synchronously are instead performed asynchronously. Command output is changed slightly to reflect that batch mode is enabled, and results are available only after batches are committed to the database. |

For operational information about the `ldapadd` command, see Chapter .

**Example**

```
ldapadd -D mail=JohnDoe@software.com -w secret -f newfile
```

This command binds the user `John Doe`, whose password is `secret`, to the directory, and uses the LDIF file named `newfile` as the source of a new entry in the Directory database.

newfile should contain a complete description of the new data object, including the parent object class. For example:

```
dn: o=<isp>, dc=<isp>, dc=com
o: <isp>
objectClass: top
objectClass: organization
```

---

**Note:** Do not use the `ldapadd` command with any LDIF file that does not contain a complete object description. If your LDIF file includes the `changetype` LDIF format, use `ldapmodify` instead. The `changetype` LDIF format looks like this:

```
dn:o=<isp>, dc=<isp>, dc=com
changetype: modify
add: organization
```

---

## ldapdelete

The `ldapdelete` command allows you to delete one or more entries from the Directory database.

---

**Note:** If you want to delete entries and also perform other operations in the same file, use the `ldapmodify` command for all of the operations.

---

The `ldapdelete` command supports UTF-8 input.

### Syntax

```
ldapdelete [-n] [-v] [-c] [-d <level>] [-f <file>] [-D <binddn>]
[-w <passwd>] [-h <host>] [-p <port>] [dn] [-g <adminGroupDN>] [-m]
```

Where:

- |                               |                                                                                                                                                                         |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-n</code>               | Shows what would be done, but doesn't actually add entries. Useful for debugging in conjunction with <code>-v</code> .                                                  |
| <code>-v</code>               | Uses verbose mode, with many diagnostics written to standard output.                                                                                                    |
| <code>-c</code>               | Continuous operation mode. Errors are reported, but LDAP continues to delete entries. The default is to exit after reporting an error.                                  |
| <code>-d &lt;level&gt;</code> | Sets the LDAP debugging level to <code>level</code> . <code>ldapdelete</code> must be compiled with <code>LDAP_DEBUG</code> defined for this option to have any effect. |

|                   |                                                                                                                                                                                                                                                                                                                 |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -f <file>         | Reads a series of lines from <code>file</code> instead of from standard input, performing one LDAP search for each line. In this case, the filter given on the command line is treated as a pattern where the first occurrence of %s is replaced with a line from file.                                         |
| -D <binddn>       | Uses <code>binddn</code> to bind to the directory. <binddn> should be a string-represented DN as defined in RFC 1779.<br>See <a href="http://www.rfc-editor.org/rfcsearch.html">http://www.rfc-editor.org/rfcsearch.html</a>                                                                                    |
| -w <passwd>       | Uses <password> as the password for simple authentication.                                                                                                                                                                                                                                                      |
| -h <host>         | Specifies an alternate host on which the LDAP server is running.                                                                                                                                                                                                                                                |
| -p <port>         | Specifies an alternate TCP port where the LDAP server is listening.                                                                                                                                                                                                                                             |
| dn                | Distinguished name of the entries to be deleted. Each dn should be a string-represented distinguished name as defined in RFC 1779.<br>See <a href="http://www.rfc-editor.org/rfcsearch.html">http://www.rfc-editor.org/rfcsearch.html</a>                                                                       |
| -g <adminGroupDN> | Specifies the distinguished name for the InterManager adminGroup that the user wants to bind as to get elevated permissions.                                                                                                                                                                                    |
| -m                | Enables batch mode. When this option is specified, all operations that this utility normally performs synchronously are instead performed asynchronously. Command output is changed slightly to reflect that batch mode is enabled, and results are available only after batches are committed to the database. |

### Example

```
ldapdelete "cn=Delete Me, o=Software.com, c=US"
```

This example deletes the entry named with common name `Delete Me` directly below the `Software.com` organizational entry.

## ldapmodify

The `ldapmodify` command allows you to modify entries to the Directory database.

The `ldapmodify` command supports UTF-8 input.

### Syntax

```
ldapmodify [-b] [-c] [-r] [-n] [-v] [-d <level>] [-D <binddn>]
[-w <passwd>] [-h <host>] [-p <port>] [-f <file>] [-g <adminGroupDN>]
[-m]
```

Where:

|                   |                                                                                                                                                                                                                                                                                                                 |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -b                | Assumes that any values that start with a '/' are binary values, and that the actual value is in a file whose path is specified in the place where values normally appear.                                                                                                                                      |
| -c                | Continuous operation mode. Errors are reported, but <code>ldapadd</code> will continue to operate with modifications. The default is to exit after reporting an error.                                                                                                                                          |
| -r                | Replaces existing values by default.                                                                                                                                                                                                                                                                            |
| -n                | Shows what would be done, but doesn't actually add entries. Useful for debugging in conjunction with <code>-v</code> .                                                                                                                                                                                          |
| -v                | Uses verbose mode, with many diagnostics written to standard output.                                                                                                                                                                                                                                            |
| -d <level>        | Sets the LDAP debugging level to <level>.                                                                                                                                                                                                                                                                       |
| -D <binddn>       | Uses <binddn> to bind to the directory. <binddn> should be a string-represented distinguished name as defined in RFC 1779.                                                                                                                                                                                      |
| -w <passwd>       | Uses <password> as the password for simple authentication.                                                                                                                                                                                                                                                      |
| -h <host>         | Specifies an alternate host on which the LDAP server is running.                                                                                                                                                                                                                                                |
| -p <port>         | Specifies an alternate TCP port where the LDAP server is listening.                                                                                                                                                                                                                                             |
| -f <file>         | Reads the entry modification information from <file> instead of from standard input.                                                                                                                                                                                                                            |
| -g <adminGroupDN> | Specifies the DN for the InterManager adminGroup that the user wants to bind as to get elevated permissions.                                                                                                                                                                                                    |
| -m                | Enables batch mode. When this option is specified, all operations that this utility normally performs synchronously are instead performed asynchronously. Command output is changed slightly to reflect that batch mode is enabled, and results are available only after batches are committed to the database. |

For operational information about the `ldapmodify` command, see Chapter .

### Example

```
ldapmodify -D mail=JohnDoe@software.com -w secret -f file2
```

This command binds the user John Doe, whose password is `secret`, to the directory, and modifies the Directory database entries specified in the LDIF file named `file2`.

file2 should use the changetype LDIF format. For example:

```
dn:o=<isp>, dc=<isp>, dc=com
changetype: modify
add: organization
```

**Note:** If you want to make several types of modifications to a single object, such as additions and deletions of attributes, use the changetype LDIF format before issuing the ldapmodify command. For example:

```
dn:o=<isp>, dc=<isp>, dc=com
changetype: modify
delete: businessCategory
-
changetype: modify
add: telephoneNumber
telephoneNumber: 1234567
```

## ldapmodrdn

The ldapmodrdn command allows you to modify the relative distinguished name (RDN) of one or more entries in the Directory database.

The ldapmodrdn command supports UTF-8 input.

### Syntax

```
ldapmodrdn [-r] [-n] [-v] [-c][<-d <level>][<-D <binddn>]
[-w <passwd>][<-h <host>] [-p <port>] [-f <file>] [dn <rdn>]
[-g <adminGroupDN>]
```

Where:

|            |                                                                                                                                        |
|------------|----------------------------------------------------------------------------------------------------------------------------------------|
| -r         | Removes the old RDN values from the entry. The default is to keep the old values.                                                      |
| -n         | Shows what would be done, but doesn't actually add entries. Useful for debugging in conjunction with -v.                               |
| -v         | Uses verbose mode, with many diagnostics written to standard output.                                                                   |
| -c         | Continuous operation mode. Errors are reported, but LDAP continues to modify entries. The default is to exit after reporting an error. |
| -d <level> | Sets the LDAP debugging level to <level>. ldapmodrdn must be compiled with LDAP_DEBUG defined for this option to have any effect.      |

|                                      |                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-D &lt;binddn&gt;</code>       | Uses <code>&lt;binddn&gt;</code> to bind to the directory. <code>&lt;binddn&gt;</code> should be a string-represented distinguished name as defined in RFC 1779. See <a href="http://www.rfc-editor.org/rfcsearch.html">http://www.rfc-editor.org/rfcsearch.html</a>                                                                                                                             |
| <code>-w &lt;passwd&gt;</code>       | Uses <code>&lt;password&gt;</code> as the password for simple authentication.                                                                                                                                                                                                                                                                                                                    |
| <code>-h &lt;host&gt;</code>         | Specifies an alternate host on which the LDAP server is running.                                                                                                                                                                                                                                                                                                                                 |
| <code>-p &lt;port&gt;</code>         | Specifies an alternate TCP port where the LDAP server is listening.                                                                                                                                                                                                                                                                                                                              |
| <code>dn &lt;rdn&gt;</code>          | Distinguished name / relative distinguished name pair for the entries to be deleted. <code>&lt;rdn&gt;</code> replaces the RDN of the entry specified by the DN, <code>&lt;dn&gt;</code> .<br>Each <code>dn</code> should be a string-represented distinguished name as defined in RFC 1779. See <a href="http://www.rfc-editor.org/rfcsearch.html">http://www.rfc-editor.org/rfcsearch.html</a> |
| <code>-g &lt;adminGroupDN&gt;</code> | Specifies the distinguished name for the InterManager adminGroup that the user wants to bind as to get elevated permissions.                                                                                                                                                                                                                                                                     |

### Example

Assume that the file `tmp/entrymods` has the following contents:

```
cn=Modify Me, o=Software.com, c=US cn=The New Me
```

In that case the following command changes the RDN of the `Modify Me` entry from `Modify Me` to `The New Me` and removes the old `cn, Modify Me`:

```
ldapmodrdn -r -f/tmp/entrymods
```

## Idapsearch

The `ldapsearch` command allows you to perform a search using a specified search filter. The filter should conform to the string representation for LDAP filters defined in RFC 1558. See <http://www.rfc-editor.org/rfcsearch.html>.

If `ldapsearch` finds one or more entries, the attributes specified by `attrs` are retrieved and the entries and values are printed to standard output. If no `attrs` are listed, all attributes are returned.

The `ldapsearch` command supports UTF-8 input.

### Syntax

```
ldapsearch [-n] [-u] [-v] [-t] [-A] [-B] [-L] [-d <level>] [-F <sep>]
[-f <file>] [-D <binddn>] [-w <passwd>] [-h <host>] [-p <port>]
[-b <"base DN">] [-s <scope>] [-a <deref>] [-l <time limit>]
[-z <size limit>] [<filter>] [<attrs>] [-g <adminGroupDN>]
```

Where:

- n                      Shows what would be done, but doesn't actually do the search. Useful for debugging in conjunction with -v.
- u                      Includes the user friendly entry names in the output.
- v                      Uses verbose mode, with many diagnostics written to standard output.
- t                      Writes retrieved values to a set of temporary files. This is useful for dealing with non-ASCII values such as jpegPhoto or audio.
- A                      Retrieves attribute names only (no values). This is useful when you want to see if an attribute is present in an entry, but are not interested in the specific values.
- B                      Does not suppress the display of non-ASCII values. This is useful when dealing with values that appear in alternate character sets such as ISO-8859.1. This option is implied by -L (see below).
- L                      Displays search results in LDIF format. This option also turns on the -B option and causes the -F option to be ignored.
- d <level>            Sets the LDAP debugging level to <level>. ldapmodrdn must be compiled with LDAP\_DEBUG defined for this option to have any effect.
- F <sep>              Uses <sep> as the field separator between attribute names and values. The default separator is =. If the -L flag is specified, this option is ignored.
- f <file>             Reads a series of lines from <file> instead of from standard input, performing one LDAP search for each line. In this case, the filter given on the command line is treated as a pattern where the first occurrence of %s is replaced with a line from <file>. If <file> is a single-character, then the lines are read from standard input.
- D <binddn>           Uses <binddn> to bind to the directory. <binddn> should be a string-represented distinguished name as defined in RFC 1779. See <http://www.rfc-editor.org/rfcsearch.html>
- w <passwd>           Uses <password> as the password for simple authentication.
- h <host>             Specifies an alternate host on which the LDAP server is running.
- p <port>             Specifies an alternate TCP port where the LDAP server is listening.

|                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-b &lt;"base DN"&gt;</code>    | Uses <code>&lt;"baseDN"&gt;</code> as the starting point for the search instead of the default.                                                                                                                                                                                                                                                                                                                                                   |
| <code>-s &lt;scope&gt;</code>        | Specifies the scope of the search. <code>&lt;scope&gt;</code> should have one of the following values:<br>base – specifies a base object search<br>one – specifies a single level search<br>sub – specifies a subtree search<br>The default is <code>sub</code> .                                                                                                                                                                                 |
| <code>-a &lt;deref&gt;</code>        | Specifies how alias dereferencing is done. <code>&lt;deref&gt;</code> should have one of the following values:<br>never – specifies that aliases are never dereferenced<br>always – specifies that aliases are always dereferenced<br>search – specifies that aliases are dereferenced when searching<br>find – specifies that aliases are dereferenced only when locating the base object for the search.<br>The default is <code>never</code> . |
| <code>-l &lt;time limit&gt;</code>   | Waits at most <code>&lt;time limit&gt;</code> seconds for a search to complete.                                                                                                                                                                                                                                                                                                                                                                   |
| <code>-z &lt;size limit&gt;</code>   | Retrieves at most <code>&lt;size limit&gt;</code> seconds for a search to complete.                                                                                                                                                                                                                                                                                                                                                               |
| <code>&lt;filter&gt;</code>          | Specifies a search filter that conforms to the string representation for LDAP filters as defined in RFC 1558.                                                                                                                                                                                                                                                                                                                                     |
| <code>&lt;attrs&gt;</code>           | Specifies the attributes to be retrieved, separated by white space. If no attribute list is given, all are retrieved.                                                                                                                                                                                                                                                                                                                             |
| <code>-g &lt;adminGroupDN&gt;</code> | Specifies the DN for the InterManager adminGroup that the user wants to bind as to get elevated permissions.                                                                                                                                                                                                                                                                                                                                      |

### Example

```
ldapsearch -D mail=JohnDoe@software.com -w secret -b "dc=software,dc=com" -s sub "(cn=Fred*)"
```

This command binds the user John Doe to the directory, and searches for everyone named Fred in the domain software.com.

# A

## ***License Information***

---

This appendix contains license information related to InterMail Mx.

### **InterMail Licensing Agreement**

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL SOFTWARE.COM BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

### **EMANATE**

InterMail incorporates the EMANATE server as part of its monitoring functionality. Software.com licenses EMANATE pursuant to a license agreement with SNMP Research International, Incorporated. The copying and distribution of EMANATE is with the permission of SNMP Research International, Incorporated.

### **GNU General Public License**

Version 2, June 1991

Copyright (C) 1991 Free Software Foundation, Inc.

59 Temple Place - Suite 330, Boston, MA 02111-1307, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the library GPL. It is numbered 2 because it goes with version 2 of the ordinary GPL.]

#### **Preamble**

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Library General Public License, applies to some specially designated Free Software Foundation software, and to any other libraries whose authors decide to use it. You can use it for your libraries, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library, or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link a program with the library, you must provide complete object files to the recipients so that they can relink them with the library, after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

Our method of protecting your rights has two steps: (1) copyright the library, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the library.

Also, for each distributor's protection, we want to make certain that everyone understands that there is no warranty for this free library. If the library is modified by someone else and passed on, we want its recipients to know that what they have is not the original version, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that companies distributing free software will individually obtain patent licenses, thus in effect transforming the program into proprietary software. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License, which was designed for utility programs. This license, the GNU Library General Public License, applies to certain designated libraries. This license is quite different from the ordinary one; be sure to read it in full, and don't assume that anything in it is the same as in the ordinary license.

The reason we have a separate public license for some libraries is that they blur the distinction we usually make between modifying or adding to a program and simply using it. Linking a program with a library, without changing the library, is in some sense simply using the library, and is analogous to running a utility program or application program. However, in a textual and legal sense, the linked executable is a combined work, a derivative of the original library, and the ordinary General Public License treats it as such.

Because of this blurred distinction, using the ordinary General Public License for libraries did not effectively promote software sharing, because most developers did not use the libraries. We concluded that weaker conditions might promote sharing better.

However, unrestricted linking of non-free programs would deprive the users of those programs of all benefit from the free status of the libraries themselves. This Library General Public License is intended to permit developers of non-free programs to use free libraries, while preserving your freedom as a user of such programs to change the free libraries that are incorporated in them. (We have not seen how to achieve this as regards changes in header files, but we have achieved it as regards changes in the actual functions of the Library.) The hope is that this will lead to faster development of free libraries.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, while the latter only works together with the library.

Note that it is possible for a library to be covered by the ordinary General Public License rather than by this special one.

**GNU LIBRARY GENERAL PUBLIC LICENSE****TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION**

This License Agreement applies to any software library which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Library General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:
  - a) The modified work must itself be a software library.
  - b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.
  - c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.
  - d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a “work that uses the Library”. Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a “work that uses the Library” with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a “work that uses the library”. The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a “work that uses the Library” uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also compile or link a “work that uses the Library” with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

- a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable “work that uses the Library”, as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)
- b) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.
- c) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.
- d) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the “work that uses the Library” must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

- 7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:
  - a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.
  - b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.
- 8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.
- 9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.
- 10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein.  
You are not responsible for enforcing compliance by third parties to this License.
- 11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or

otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.
13. The Free Software Foundation may publish revised and/or new versions of the Library General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and “any later version”, you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

#### **NO WARRANTY**

BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING

ING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

## Oracle

Oracle Programs are the proprietary products of Oracle and are protected by copyright and other intellectual property laws. Customer acquires only the right to use Oracle Programs and does not acquire any rights, express or implied, in Oracle Programs or media containing Oracle Programs other than those specified by License. Oracle, or its licensor, shall at all times retain all rights, title, interest, including intellectual property rights, in Oracle Programs and media.

## The Regents of the University of California Copyright

InterMail includes software that is copyright © 1990, 1993, 1994, The Regents of the University of California. All rights reserved.

This code is derived from software contributed to Berkeley by Mike Olson.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Re-distributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Re-distributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: This product includes software developed by the University of California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

## The Regular Expression Routines

1. Permission is granted to anyone to use this software for any purpose on any computer system, and to alter it and redistribute it, subject to the following restrictions:
2. The author is not responsible for the consequences of use of this software, no matter how awful, even if they arise from flaws in it.
3. The origin of this software must not be misrepresented, either by explicit claim or by omission. Since few users ever read sources, credits must appear in the documentation.

4. Altered versions must be plainly marked as such, and must not be misrepresented as being the original software. Since few users ever read sources, credits must appear in the documentation.
5. This notice may not be removed or altered.

## **RSA Data Security, Inc. MD5 Message-Digest Algorithm**

License to copy and use this software is granted provided that it is identified as the “RSA Data Security, Inc. MD5 Message-Digest Algorithm” in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as “derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm” in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided “as is” without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.

# Glossary

---

## ***attribute***

Information describing one trait of a directory object. Each attribute has a name followed by one or more values. For example, the attribute `o`, belonging to the object class `organization`, could have the value `Software.com`. The attribute `ou`, belonging to the object class `organizationalUnit`, could have the value `engineering`.

## ***attribute value***

The data associated with an attribute. For example, `555-1212` is an attribute value for the attribute `telephoneNumber`. Some attributes are single-valued and some are multiple-valued.

## ***consumer server***

The destination server for replicated data. In InterMail, the consumer server is the Directory Cache server.

## ***class of service***

A set of permissions, resource limits, and default user preferences shared by a set of accounts that determines, among other things, the services that the users of each associated account may access. Each permission, resource limit, and preference is represented by a specific class of service attribute.

## ***class-of-service attribute***

An attribute of a class-of-service entry in the directory. Each class-of-service attribute defines a permission, resource limit, or preference that affects the set of accounts associated with the class of service.

## ***Directory Cache server***

A component of the Integrated Services Directory (ISD) that contains a copy of all or part of the master Directory database in its local cache database. The Directory Cache server is capable of servicing the same read and write requests as the Directory server, and is regularly updated from the Directory server, preventing bottlenecks to the master Directory database and ensuring quick response time to queries by other servers.

### **Directory database**

A single Oracle relational database that is the authoritative master version of InterMail account information, including an end user's domain, username, password, class of service, e-mail address, and delivery information. Directory Cache servers communicate with the Directory server, which in turn accesses the Directory database, to get the updates to their local cache databases. The Directory database is a component of the ISD, together with the Directory server, Directory Cache servers, and Directory Cache databases.

### **Directory Information Tree (DIT)**

An LDAP term for the hierarchical structure that contains all directory entries. Each directory entry is uniquely identified by a distinguished name (DN), which is a path in the DIT used to name and locate the entry, similar to a file's path in a file system.

### **Directory server**

The component of the ISD that maintains an authoritative master copy of the Directory database. It contains Oracle client libraries to communicate with the Directory database and is responsible for storing replication information that is read by the Directory Cache servers.

### **distinguished name (DN)**

An LDAP term for a name of a directory entry that uniquely identifies the entry by providing a complete pathname through the DIT, analogous to a filename composed of a path of directory names in an operating system.

#### **Example:**

dn: uid=johndoe, ou=engineering, dc=software, dc=com

### **DIT**

See *Directory Information Tree*.

### **DN**

See *distinguished name*.

### **domain**

One or more IP addresses corresponding to a particular organization. For example, `software.com` is a domain that contains addresses in the 10.2.6.x Class C IP network.

### **entry**

The basic unit of information stored in a directory. Entries consist of a collection of attributes.

### **failover server**

A server that assumes the identity of a failed server so that the information from the failed server remains accessible.

**LDAP (Lightweight Directory Access Protocol)**

An Internet protocol that allows users to access and search a variety of otherwise incompatible directory systems for information.

**LDIF (LDAP Data Interchange Format)**

A standard way of representing directory data in a text file format, used to import and export data to and from LDAP directories. An LDIF entry consists of a series of lines of ASCII text, the first line specifying a distinguished name for the entry, and each subsequent line specifying an attribute of the entry.

**Example:**

This is an LDIF entry for a Software.com employee named John Doe:

```
dn: uid=johndoe, dc=software, dc=com
uid: johndoe
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: mailUser
objectClass: mailUserPrefs
cn: John Doe
sn: Doe
mail: john.doe@software.com
mailForwarding: F
```

**leaf node**

A location in a DIT that is at the end of a branch. A leaf node has no descendants.

**matching rule**

A rule determining how attribute values of a specified syntax are compared during search, modify, add, and delete operations. For example, the matching rule `caseIgnoreMatch` means that uppercase and lowercase letters are treated the same way.

**object class**

A collection of required and optional attributes in a directory that defines a type of data. For example, `person`, `organization`, and `domain` are standard object classes in an LDAP directory.

**object identifier (OID)**

A string of numbers separated by dots used to uniquely identify objects in the directory. Each part of an OID represents a node in a hierarchical OID tree. This allows blocks of namespace to be delegated to individual organizations for their own use.

For example, the InterMail object class `mailUserPrefs` is the string of numbers assigned to Software.com by the Internet Engineering Task Force, `1.3.6.1.4.1.2415`, followed by a string of numbers designated by

Software.com, 1.2.2.6. This creates an OID of 1.3.6.1.4.1.2415.1.2.2.6 for the object class mailUserPrefs.

***partitioning***

The process of replicating different portions of the Directory database to different Directory Cache servers.

***relative distinguished name (RDN)***

An LDAP term for the most specific component of a distinguished name. An RDN must be unique among entries of the same parent in the DIT.

***replica set***

A set of identical Directory Cache servers that are interchangeable for the purpose of satisfying client requests. If one of these servers is unavailable, a client tries to communicate with the others, one at a time. Replica sets thereby function as a failover mechanism.

***replication***

The process by which directory entries are automatically copied from the Directory server to one or more Directory Cache servers for local storage.

***replication agreement***

A filter that specifies which Directory database entries and their attributes are copied and maintained by a particular Directory Cache server.

***replication area***

A set of objects and attributes to be replicated to a consumer server.

***RFC (Request For Comments)***

One of a series of documents published by the Internet Engineering Task Force (IETF), which sets the standards for the Internet. LDAPv3 standards may be found in RFC 2251 through RFC 2256. The URL is <http://www.rfc-editor.org/rfcsearch.html>.

***RME (Remote Method Execution)***

The protocol that InterMail servers use to communicate the results of transactions between themselves.

***schema***

A description of the Directory database that sets the rules for what can be stored in it, as well as how the Directory server and its clients are to treat information during search, modify, add, or delete operations. In LDAP-based directories, a schema is composed of object classes and attributes.

***supplier server***

A server that supplies information to be replicated. In InterMail, the supplier server is the Directory server.

***syntax***

A description of the type of data contained in an attribute. Boolean, Directory string, and Integer are three types of syntaxes.



# Index

---

## A

- abstract object classes, 62
- account information, 1
- account provisioning, writing to the Directory server during, 9
- account status, setting, 257
- accounts
  - changing the addresses of, 255
  - commands relating to, 247
  - creating
    - with imdbcontrol, 247, 248
    - with imldapsh, 277
  - defining class of service attributes for, 255
  - deleting
    - with imdbcontrol, 248
    - with imldapsh, 278
  - deleting class of service attributes from, 249
  - deleting forwarding addresses from, 261
  - disabling forwarding for, 261
  - disabling local delivery for, 262
  - enabling auto-reply for, 257
  - enabling forwarding for, 262
  - enabling local delivery for, 263
  - forwarding mail from, 260
  - listing forwarding addresses for, 263
  - modifying, 253
  - setting login names for, 254
  - setting passwords for, 259
  - setting quota values for, 256
  - summarizing in a report, 236
  - viewing information on, 249, 251, 252
- ACI (Access Control Information) filters, 4, 7
  - ACI (Access Control Information) rules, 75
    - overview of, 9
    - usage of, 10
  - adminAllocation object class, 101
  - adminAllocCounts object class, 102
  - adminGroup object class, 103
  - adminPolicy object class, 103
  - adminRealm object class, 104
  - adminRealmSpec object class, 105
  - adminRole object class, 105
  - adminRoot object class, 106
  - adminTarget object class, 106
  - adminUserPrefs object class, 107
  - alias addresses
    - creating, 264
    - deleting, 265
    - listing, 265
  - alias object class, 107
  - alias queries, 22
  - allocation rules, 75
  - anonBindAccess configuration key, 188
  - anonymous binding, 4
  - application partitioning, 36
    - example of, 57
  - applicationEntity object class, 107
  - applicationProcess object class, 108
  - architecture, distributed, 3
  - attribute constraints, 73
  - attribute indexing, 75
  - attribute values, term defined, 297
  - attributeAliasingEnable configuration key, 189

attributes, 99  
  ACI rules and, 75  
  allocation rules and, 75  
  chaining and, 41  
  class of service  
    adding to the mailLocalUserPrefs object  
      class, 71  
    defining values for, 255  
    deleting, 249, 268  
    retrieving, 251  
  defined, 128  
  defining, 67  
  indexed, file structure for, 20  
  listing, 251  
  listing of, 129  
  matching rules for, 66  
  new  
    adding to an object class, 69  
    adding to the schema, 68  
  overview of, 65  
  standard object classes and, 59, 67  
  syntax of, 66  
    rules for, 66  
  term defined, 297  
  viewing, 249  
attributeSelection configuration key, 42, 43, 189  
authoritative mode, of Directory Cache server, 17  
auto-reply feature, enabling, 257  
auto-reply messages, setting location of, 258  
auxiliary object classes, 61, 63

## C

cacheAlwaysReadThru configuration key, 190  
cacheAuthoritativeForMTA configuration key, 191  
cacheAuthoritativeOnDbFail configuration key, 191  
cacheDisableReadThrus configuration key, 192  
cacheDisableWriteThrus configuration key, 193  
cacheReReadInterval configuration key, 193  
certificationAuthority object class, 108  
certificationAuthority-V2 object class, 109  
chaining  
  Directory Cache server and, 40  
  replication agreement using, sample, 47  
chainingInfo configuration key, 41, 44, 194  
change logs  
  on the Directory server, 11  
  replication agreements and, 40  
changeLog configuration key, 194  
changeLogEntry object class, 109

checkPointInterval configuration key, 195  
checkPointRetryInterval configuration key, 195  
chgLogPageSize configuration key, 196  
class of service attributes  
  adding to the mailLocalUserPrefs object  
    class, 71  
  defining values for, 255  
  deleting, 249, 268  
  retrieving, 251  
  term defined, 297  
class of service operations, 266  
classes of service  
  creating, 266  
  deleting, 266  
  deleting attributes from, 268  
  listing, 267  
  listing attributes of, 267  
  setting attributes for, 267  
  term defined, 297  
client queries  
  LDAP, 23  
  replication design and, 40  
compatibleQuotaKbytesConversion  
  configuration key, 196  
Configuration database, replication agreements  
  and, 40  
configuration keys, 185  
  *See also individual configuration keys*  
  for Directory Cache server, 24  
  for Directory server, 12, 24  
  for replication agreements, 42  
  impact of changes to, 187  
  sample, 185  
  setting, 187  
consumer servers, 39  
  term defined, 297  
country object class, 109  
CreateAccount option, 247  
CreateAlias option, 264  
CreateCos option, 266  
CreateDomain option, 242  
createEntryAudit configuration key, 196  
CreateRemoteForward option, 260  
cRLDistributionPoint object class, 110

## D

data partitioning. *See* partitioning  
data, exporting to LDIF, 278  
dbLogFileMaxSizeKb configuration key, 20, 197  
dbSuppressFsync configuration key, 197  
dcObject object class, 110

- defaultBindDN configuration key, 198
- defaultBindPassword configuration key, 198
- defaultChangelogTablespace configuration key, 199
- defaultDirServer configuration key, 23, 199
- DeleteAccount option, 248
- DeleteAccountCos option, 249
- DeleteAlias option, 265
- DeleteCos option, 266
- DeleteDomain option, 243
- DeleteRemoteForward option, 261
- device object class, 110
- dirCachePort configuration key, 200
- Directory Cache database
  - chaining and, 40
  - copying, 21
  - file for, 20
  - initializing, 21
  - other ISD components and, 3
  - read requests and, 19
  - read-through requests and, 19
  - replica sets and, 46
  - replication agreements and, 40
  - updates to, 11, 18, 20
- Directory Cache server
  - architecture of, 17
  - assigning to RME or LDAP clients, 44
  - authoritative mode of, defined, 17
  - bypassing communication with, 9
  - chaining and, 40, 47
  - communications protocols and, 22
  - configuration keys for, 24
    - for replication agreements, 42
  - directory schema and, 99
  - file structure on, 20
  - non-authoritative mode of
    - defined, 17
    - queries and, 23
  - operation of, 21
  - other ISD components and, 2
  - partitioning of data on, 36
  - read requests to, 8, 19
  - read-through requests from, 8, 19
  - replica sets and, 46
  - replication agreements and, 39, 75
  - replication of data to, 35
  - schema changes and, 74
  - statistics files for, 31
  - synchronization of, with Directory server, 18, 20
    - term defined, 297
    - write-through requests from, 19
- directory data
  - accessing, 4
  - replication of, 18
- Directory database
  - See also* ISD
  - access to, 23
  - Directory Cache server and, 17
  - directory schema and, 99
  - DIT and, 77
  - effect of replication agreements on, 75
  - modifying, 238
  - other ISD components and, 2
  - replicating, 44
  - schema checking and, 74
  - term defined, 298
- directory information
  - partitioning of, 18, 36
  - replication of, 35
- directory management utilities, 235
- directory schema, 59, 99
  - adding new attributes to, 68
  - object classes in, 60
- Directory server, 7
  - architecture of, 7
  - change log on, 11
  - configuration keys for, 12, 24
  - Directory Cache server and, 17
  - directory schema and, 99
  - information flow through, 8
  - other ISD components and, 2
  - read requests to, 8
  - read-through requests to, 8, 19
  - replication of data from, 35
  - schema checking and, 74
  - statistics files for, 15
  - synchronization of Directory Cache server
    - with, 20
    - term defined, 298
    - write-through requests to, 9, 19
- dirRmeConnections configuration key, 200
- dirRmeHost configuration key, 200
- dirRmeHosts configuration key, 36, 44, 201
- dirRmeMaxSecondaryCalls configuration key, 201
- dirRmePort configuration key, 202
- DisableForwarding option, 261
- DisablePOPDelivery option, 262
- distinguished name syntax type, features of, 129

distinguished names, 77  
    term defined, 298

distributed architecture, 3

DIT (Directory Information Tree), 77  
    initial, 77  
    modifying, 271  
    term defined, 298

dmd object class, 111

domain object class, 112

domains  
    changing the type of, 246  
    commands related to, 242  
    creating, 242  
    default, getting, 244  
    deleting, 243, 253  
    listing, 244  
    term defined, 298

dsA object class, 113

**E**

EnableForwarding option, 262

EnablePOPDelivery option, 263

entry, term defined, 298

expChgLogCommitSize configuration key, 202

**F**

failover capability, partitioning and, 36

failover server, term defined, 298

forwarding addresses  
    creating, 260  
    deleting, 261  
    listing, 263

forwarding, disabling, 261

**G**

GetAccount option, 249

GetAccountCos option, 251

GetAccountFull option, 251

GetDefaultDomain option, 244

GetPassword option, 251

groupOfNames object class, 114

groupOfUniqueNames object class, 114

**I**

IETF (Internet Engineering Task Force), 300

imcacheread command, 237

imdbcontrol command  
    account operations with, 240, 247  
    class of service operations with, 241, 266

    compared with imldapsh, 276

    domain operations with, 239, 242

    mail delivery operations with, 241

    options for, 239  
        *See also individual options*

    SMTP alias operations with, 241, 264

    syntax of, 238

imdircachesserv process, 17

imdirmake command, 21, 74, 268

imdirprobe command, 269

imdirsrv process, 7

imdirsync command, 21, 270  
    replication agreements and, 40

imdirupdate command, 270

imldapsh command, 238, 271  
    compared with imdbcontrol, 276  
    options for, 272  
    variables in, 276

imldifexport command, 278

impwdhash command, 279

indexed attributes  
    *See also* attribute indexing  
    chaining and, 41

indexThreadSnoozePeriod configuration key, 203

inetOrgPerson object class, 115  
    position in hierarchy, 61

initIndicesFallback configuration key, 203

InterMail servers, process names for, 186

IP addresses  
    in configuration keys, 188  
    restricting, 4

ISD (Integrated Services Directory)  
    *See also* Directory database  
    adding new entries to, 280  
    components of, 1  
    deleting entries from, 282  
    modifying entries in, 271, 283, 285  
    object classes in, 60  
    role of, 1  
    searching, 271, 286  
    updating, 270

**L**

LDAP attributes, 65

LDAP clients  
    access to Directory database by, 23  
    assigning Directory Cache servers to, 44  
    read-through operations and, 19

LDAP data model, overview of, 4

- LDAP entries
    - checking, 74
    - files for, 20
    - for replication agreements, 40
  - LDAP object classes, 60
  - LDAP protocol, Directory Cache server and, 17, 23
  - LDAP queries, 23
    - chaining and, 41
  - LDAP schema, location of, 59
  - LDAP standards, 6
  - LDAP, term defined, 299
  - ldapAccessList configuration key, 204
  - ldapACICacheMaxCount configuration key, 204
  - ldapACICacheMaxSizeKB configuration key, 204
  - ldapadd command, 280
  - ldapAllocRootOverride configuration key, 205
  - ldapAllowRuleDN configuration key, 205
  - ldapAsyncOperation configuration key, 206
  - ldapAsyncSearch configuration key, 207
  - ldapBackend configuration key, 207
  - ldapBatchTimeoutMS configuration key, 208
  - ldapBindThruEnable configuration key, 209
  - ldapClientTimeout configuration key, 209
  - ldapConfigDn configuration key, 210
  - ldapCosCacheMaxCount configuration key, 210
  - ldapCosCacheMaxSizeKb configuration key, 210
  - ldapDbEntryCacheSizeInKB configuration key, 211
  - ldapDBEntryPageSizeInKB configuration key, 211
  - ldapDBIndexCacheSizeInKB configuration key, 212
  - ldapDBIndexPageSizeInKB configuration key, 212
  - ldapDebugWriteEnable configuration key, 213
  - ldapdelete command, 282
  - ldapEnableAutoAdminGroup configuration key, 214
  - ldapEntryCacheMaxCount configuration key, 214
  - ldapEntryCacheMaxSizeKb configuration key, 215
  - ldapIndices configuration key, 215
  - ldapIndicesConfigRdn configuration key, 217
  - ldapMasterHosts configuration key, 217
  - ldapMaxBatchOperations configuration key, 217
  - ldapmodify command, 283
  - ldapmodrdn command, 285
  - ldapNumEntryDbFiles configuration key, 20, 218
  - ldapNumIndexDbFiles configuration key, 20, 218
  - ldapOperationLimit configuration key, 219
  - ldapPort configuration key, 219
  - ldapReplicationAgreement configuration key, 42, 44, 219
  - ldapRootDn configuration key, 220
  - ldapRootPwd configuration key, 220
  - ldapSchemaCheck configuration key, 74, 221
  - ldapSchemaDn configuration key, 221
  - ldapSchemaFile configuration key, 222
  - ldapsearch command, 286
  - ldapServerHosts configuration key, 36, 44, 222
  - ldapSizeLimit configuration key, 223
  - ldapTimeoutLimit configuration key, 223
  - LDIF
    - exporting data to, 279
    - term defined, 299
  - lead node, term defined, 299
  - ListAccountForwards option, 263
  - ListAccounts option, 252
  - ListAliases option, 265
  - ListCosNames option, 267
  - ListDomains option, 244
  - load balancing, partitioning and, 36
  - local delivery
    - disabling, 262
    - enabling, 263
  - logAgeHours configuration key, 11, 224
  - logExpireHours configuration key, 224
  - loginAliases configuration key, 225
  - loginFilter configuration key, 226
  - logNumTablesLimit configuration key, 227
- M**
- mail forwarding, enabling, 262
  - mailDomain object class, 117
  - mailLocalUserPrefs object class, 117
    - adding attributes to, 67
    - adding class-of-service attributes to, 71
  - mailUser object class, 117
  - mailUserPrefs object class, 118
  - masterSearchRoot configuration key, 227
  - matching rules, 66
    - term defined, 299
  - maxCursorsPerConn configuration key, 228
  - mix-in object classes. *See* auxiliary object classes
  - ModifyAccount option, 253
  - ModifyAccountPop option, 254
  - ModifyAccountSmtP option, 255
  - modifyEntryAudit configuration key, 228
  - multi-threading, 23

## N

- non-authoritative mode, of Directory Cache server, 17
  - queries and, 23
- numLdapConnections configuration key, 229

## O

- object classes, 60
  - abstract, 62
  - ACI rules and, 75
  - adding new attributes to, 68, 69
  - auxiliary, 61, 63
  - creating, 61, 63
  - definition of, 100
  - described, 99
  - hierarchy of, 61
  - LDAP, 60
  - standard, modifying, 59, 67
  - structural, 62
  - term defined, 299
- object identifiers (OIDs), term defined, 299
- object partitioning, 36
- oracleConnectWait configuration key, 229
- oracleMaxOperationTime configuration key, 229
- organization object class, 120
- organizationalPerson object class, 121
  - position in hierarchy, 61
- organizationalRole object class, 122
- organizationalUnit object class, 123

## P

- partition configuration key, 42, 43, 229
- partition object class, 124
- partitioning, 36
  - chaining and, 41
  - configuration keys for, 42
  - example of, 49, 52, 55
  - with multiple replication agreements, 50
  - overview of, 3, 18
  - replica sets and, 53
  - term defined, 300
- passwords
  - hashing, 279
  - setting, 259
  - viewing, 251
- person object class, 125
  - position in hierarchy, 61
- POP login names, setting, 254
- POP queries, 22

- primaryDbNumConnections configuration key, 230
- proxy hosts, setting, 259

## Q

- quota values, setting, 256

## R

- read requests
  - to Directory Cache server, 19
  - to Directory server, 8
- read-through requests
  - from Directory Cache server, 19
  - to Directory server, 8, 19
- relative distinguished names, 77
  - modification of, 285
  - term defined, 300
- replAgreement object class, 125
- replAreaSpec configuration key, 42, 44, 231
- replica sets
  - described, 35
  - partitioning and, 53
  - replication agreement using, sample, 46
  - term defined, 300
- replication
  - See also* replication agreements
  - designing, 37
  - overview of, 3, 18, 35
  - term defined, 300
- replication agreements, 75
  - chaining in, 40
  - changing, 40
  - configuration keys for, 42
  - creating, 43
  - default, 45
  - overview of, 39
  - sample, 44
  - storage of, 40
  - term defined, 300
- replication areas
  - specifying, 42
  - term defined, 300
- residentialPerson object class, 126
- RFC (Request for Comments), term defined, 300
- RME clients
  - assigning Directory Cache servers to, 44
  - read-through requests and, 19
- RME protocol
  - Directory Cache server and, 17, 22
  - term defined, 300

RME queries, 22  
  chaining for, 41  
rootBindAccess configuration key, 231  
routing attributes, chaining and, 41

## S

scalability features, 3  
scConfig object class, 127  
scConfigRoot object class, 127  
schema attributes. *See* attributes  
schema checking, 74  
  limitations of, 74  
schemas  
  matching rules in, 66  
  term defined, 300  
security features, 4  
servers  
  process names for, 186  
  setting configuration keys for, 187  
SetAccountCos option, 255  
SetAccountQuota option, 256  
SetAccountStatus option, 257  
SetAutoReply option, 257  
SetAutoReplyHost option, 258  
SetCosAttribute option, 267  
SetPassword option, 259  
SetProxyHosts option, 259  
SetWildcardAccount option, 245  
ShowCos option, 267  
SMTP alias operations, 264  
SMTP queries, 22  
standard object classes, modifying, 67  
statistics files  
  Directory Cache server, 31  
  Directory server, 15

structural object classes, 61, 62  
subschema object class, 127  
supplier servers, 39  
  term defined, 300  
synchronization  
  of databases, 270  
  of servers, 20  
syntax rules, 66  
syntax, term defined, 301  
system scalability  
  chaining and, 40  
  partitioning and, 36

## T

top object class, 128  
  position in hierarchy, 61

## U

UnsetCosAttribute option, 268  
UnsetWildcardAccount option, 245  
UpdateDomain option, 246  
updateThreadRetryPeriod configuration key, 232  
users, printing information about, 237  
userSecurityInformation object class, 128

## W

wildcard account  
  disabling, 245  
  setting, 245  
write requests, direct, 9  
writeChangeLog configuration key, 232  
write-through requests, to Directory server, 9, 19

