Sun Internet Mail Server™ 4.0 Administrator's Guide

THE NETWORK IS THE COMPUTER™

A Sun Microsystems, Inc. Business
901 San Antonio Road
Palo Alto, CA 94303 USA
650-960-1300 fax 650-969-9131

Part No.:805-7676-10
Revision A, July 1999

Please
Recycle

Adobe PostScript

Contents

Figures

Tables

Preface

SIMS System Administration Guide begins where *SIMS Installation Guide* ends. Use this guide in conjunction with *SIMS Reference Manual* to fine-tune the default configuration, and to maintain, monitor, and troubleshoot your mail server after installing the software and loading the user and distribution lists from your existing email system.

SIMS User Registration

Register as a user of the Sun Internet Mail Server 4.0 (SIMS) to receive information about new releases, upgrade offers, and promotions. To register, press the *Registration* button at the Administration Console login page. Fill in the form requesting your name, address, email address, and other information, and press *Send*. When Sun receives the completed registration form, you will receive an email acknowledgment. You must provide an email address in order to receive a confirmation notice.

Error Conditions

Registration errors are rare, but Table P-1 describes the possible error messages and the required action.

TABLE P-1 Registration Error Conditions and Required Action

Error Message	Required Action
"The server could not set a locale to encode the mail. There was no locale supplied and the server could not set the default properly."	Make sure that you start registration from the Admin Console screen.
"The server could not obtain the <LOCALE> locale that you registered from to properly format the mail. It is necessary to have the same locale installed on the server that you registered from."	Either make sure the locale installed on server is the same as the locale you are registering from on your client, or type in registration in `us-ascii`.
"The mail program on the server could not be opened."	There was an error involving the `sendmail` program. Make sure that `/usr/lib/sendmail` is on your system and properly configured.
"There was not enough memory to process the mail."	You've run out of swap space. Shut down applications or increase swap and try again.

Who Should Use This Book

This book is intended for two audiences:

- Highly technical network administrators who are experienced in working with Solaris™ systems and who manage a network comprised of Sun™ workstations, personal computers (PCs), Macintoshes, or IBM mainframes that share resources. This network administrator has previous experience planning, installing, configuring, maintaining, and troubleshooting an enterprise email system.
- Moderately technical network administrators with some Solaris experience who manage a network that includes Sun workstations, PCs, and Macintoshes that share resources. This network administrator may not have previous experience planning, installing, configuring, maintaining, and troubleshooting an email system.

Before You Read This Book

Before performing the tasks described in this book, you should have installed the mail server software and loaded the users and distribution lists from your existing email system if applicable per information provided in the *Sun Internet Mail Server 4.0 Installation Guide*.

How This Book Is Organized

Chapter 1, "SIMS Administration Road Map," provides an approach to thinking about SIMS administration.

Chapter 2, "The SIMS Administration Console Overview," provides overview information on the Administration Console as well as a road map for Admin Console documentation.

Chapter 3, "User/Group Management" describes how to add, delete, or modify user, group, or organizational units in the Directory Service.

Chapter 4, "Hosted Domains" describes how to create, delete, and modify hosted domains, how to create and remove hosted domain delegated administrators, and how to customize the Delegated Admin Console.

Chapter 5, "Internet Message Transport Agent (IMTA) Administration" provides step-by-step instructions for changing the message transport characteristics of SIMS.

Chapter 6, "IMTA Security and Unsolicited Bulk Email (UBE) Handling

Chapter 7, "Message Store Administration" describes step-by-step instructions for changing the Sun Message Store characteristics of SIMS.

Chapter 8, "Sun Directory Services Administration" provides limited information on directory services. References Sun and Netscape Directory Services documentation.

Chapter 9, "Populating SIMS with Users and Groups" describes how to populate users and groups from your current directory database to the SIMS directory.

Chapter 10, "Secure Sockets Layer (SSL) Support in SIMS," describes how to use the SSL security features supported by SIMS.

Chapter 11, “SIMS Periodic Maintenance Procedures,” provides procedures and background concepts that enable you to perform scheduled or as-needed maintenance.

Chapter 12, “SIMS Monitoring and Logging” describes SIMS monitoring and logging.

Chapter 13, “SIMS Troubleshooting,” describes tools that enable you to troubleshoot your mail server, and provides some troubleshooting procedures.

Appendix A, “Configuring SIMS as a Proxy Message Access Server,“describes SIMS message access proxy.

Appendix B, “Replication Configuring—Examples,” provides examples of how to configure replication.

Appendix B, “Migrating Mailboxes from /var/mail to SIMS” describes how to migrate mailboxes from /var/mai/ to SIMS.

Appendix C, “Populating the Directory Examples,” describes three examples of populating the directory.

Appendix D, “Error Messages” lists error messages and the appropriate actions.

“Glossary” lists words and phrases found in this book and their definitions.

Related Information

The following books are related to Sun Internet Mail Server 4.0. Included in this documentation set are:

- *Sun Internet Mail Server 4.0 Concepts Guide* – Provides a conceptual understanding of the SIMS product. By understanding how SIMS works on a conceptual level, readers will more easily understand the administrative tasks described in the *SIMS System Administration Guide* and *SIMS Reference Manual*.
- *Sun Internet Mail Server 4.0 Provisioning Guide* – Describes how to provision the SIMS LDAP directory with users, distribution lists, administrators, and domains by creating and importing LDIF records.
- *Sun Internet Mail Server 4.0 Advanced Installation Guide* – Describes the planning and installation procedures for the Sun Internet Mail Server (SIMS) 3.5 software on Solaris SPARC and Intel-based x86 systems. In particular, it describes the installation of the software using the Graphical User Interface (GUI).
- *Sun Internet Mail Server 4.0 Administrator’s Guide* – Describes how to fine-tune the default configuration, and maintain, monitor, and troubleshoot your mail server using the Administration Console, a GUI.

- *Sun Internet Mail Server 4.0 Reference Manua*l – Provides in-depth information about Sun Internet Mail Server. Many administrative functions can also be accomplished through command line utilities. Other advanced functions can be accomplished only through these utilities and by editing configuration files.
- *Sun Internet Mail Server 4.0 Delegated Management Guide* – Describes the SIMS Delegated Management Console and the tasks associated with the console. In particular, it describes how a delegated administrator for a hosted domain performs tasks on users and distribution lists.
- Reference manual pages (man pages) – Describes command-line utilities and detailed information about the arguments and attributes relevant to each command.
- *Sun Directory Services 3.1 Administration Guide* (http://docs.sun.com:80/ab2/coll.297.1/@Ab2CollToc?subject=sysadmin) - Describes the Sun Directory Services.
- *Netscape Directory Services documentation* (http://home.netscape.com/eng/server/directory/) - Describes the Netscape Directory Services.
- *Web Access Administrator's Guide* – Describes the core system administration tasks for the Sun Web Access software.
- Sun Internet Mail Server 4.0 Release Notes – Covers open issues and late-breaking installation, administration, and reference information that is not published in the product books.
- Sun Internet Mail Server 4.0 Web site (located at `http://www.sun.com/sims`) offers up-to-date information on a variety of topics, including:
  - On-line product documentation and late-breaking updates
  - Data sheets and evaluation guide
  - Technical white papers
  - Product demos
  - Press coverage and customer success stories
  - Client solutions

What Typographic Changes Mean

The following table describes the typographic changes used in this book.

TABLE P-2 Typographic Conventions

Typeface or Symbol	Meaning	Example
`AaBbCc123`	The names of commands, files, and directories; on-screen computer output.	Edit your `.login` file. Use `ls -a` to list all files. `machine_name% You have mail.`

`AaBbCc123`	What you type, contrasted with on-screen computer output.	`machine_name%` **`su`**
		`Password:`

AaBbCc123	Command-line place holder: replace with a real name or value.	To delete a file, type `rm` *filename*.
AaBbCc123	Book titles, new words or terms, or words to be emphasized.	Read Chapter 6 in *User's Guide*. These are called *class* options. You *must* be root to do this.

Path Convention for Screen Navigation

The following is an example of a navigation path. Navigation paths are shown at the beginning of each task. The navigation path is used in the Admin Console graphical user interface to move from the main Admin Console screen to the screen where the task is performed.

AdminConsole>Sun Message Store>Purge Options

Using the navigation path above, begin at the main Admin Console screen, shown immediately after login. Then, click on Sun Message Store to view the next screen. Written directions accompanying the path direct you to click on the Purge Option listing of the Sections List. Follow the written instructions for configuring the purge options.

Shell Prompts in Command Examples

The following table shows the default system prompt and superuser prompt for the C shell, Bourne shell, and Korn shell.

TABLE P-3 Shell Prompts

Shell	Prompt
C shell prompt	`machine_name%`
C shell superuser prompt	`machine_name#`
Bourne shell and Korn shell prompt	`$`
Bourne shell and Korn shell superuser prompt	`#`

Note – Although the majority of commands can be run without special superuser permissions, some commands can be performed only as `root`. These commands include: `imta dirsync, imta start, imta stop,` and `imta restart`. Other commands that require `root` privileges are noted within the document.

Graphical User Interface Conventions

This section describes terminology and other conventions used when discussing the Administration Console, a graphical user interface.

Terminology

The following table defines terms used in procedures associated with the Administration Console.

TABLE P-4 Graphical User Interface Terminology

Term	Explanation	Example
Check box	A yes/no or on/off control. A square box that appears highlighted and pushed in when on or pushed out when off. Usually, all check boxes in a group can be selected.	To enable the logging of each message, click the check box.
Radio button	A yes/no or on/off control. A diamond or circle that appears highlighted and pushed in when on or pushed out when off. Usually, only one radio button in a group can be selected.	You can enable the channel to ignore nonstandard encoding headers by clicking the appropriate radio button.
Click	Press and release a mouse button without moving the pointer.	Click the radio button.
Double-click	Click a mouse button twice quickly without moving the pointer.	Double-click the SMTP channel name from the list of channels to display the SMTP property book.

Notice

To better illustrate the process being discussed, SIMS manuals contain examples of data that might be used in daily business operations. The examples might include names of individuals, companies, brands, and products. SIMS manuals use only fictitious names, and any similarity to the names of individuals, companies, brands, and products used by any business enterprise is purely coincidental.

CHAPTER 1

SIMS Administration Road Map

Every organization needs to plan and implement SIMS administration procedures that are customized to their individual situation. This chapter provides some guidelines about how to think about SIMS administration. It is not meant to a complete step-by-step planning guide, but may be useful in determining how to approach the problem of administering your mail system.

At this point in your installation process we assume you have completed the planning and architectural design of your email system. We assume that you have decided on an architecture—how many and what type of servers you will need to support your email needs—and how those systems will be connected and configured. See the *SIMS Concepts Guide* for information on various email architectures and topologies.

The SIMS administration tasks are divided into three categories:

- Defining SIMS Operational Processes and Procedures.
- Going from installation to getting on-line.
- On-going SIMS administration procedures.

The following sections list some major tasks with references to further information.

Defining SIMS Operational Processes and Procedures

These tasks consists of processes to plan and consider before actual implementation.

- Define an initial user provisioning plan. How to migrate your current email users into the SIMS directory? How to migrate existing mailboxes into the Sun Message Store?
    - *SIMS Provisioning Guide.*

    - *SIMS Reference Manual*, Chapter3, Directory Information Tree and Schema.
    - Chapter 3, User/Group Management”.
    - “Migrating Mailboxes from /var/mail to SIMS” on page 315.
- Define a daily provisioning process--how will new users, groups, and hosted domains be added, modified, and removed.
    - *SIMS Provisioning Guide*.
    - *SIMS Reference Manual*: Chapter 3, Directory Information Tree and Schema.
    - Chapter 3, User/Group Management.
    - Chapter 4, Hosted Domains.
- Define a directory backup plan.
    - Sun Directory Services documentation (http://docs.sun.com:80/ab2/coll.297.1/@Ab2CollToc?subject=sysadmin).
    - Netscape Directory Services documentation (http://home.netscape.com/eng/server/directory/).
- Define a message store backup plan.
    - “Message Store Backup and Restore” on page 237.
- Define a system monitoring plan.
    - “SIMS Monitoring Plan” on page 261.
- Define your LDAP directory design. That is, what are the names of the domains that you will support and how will they be reflected in the directory information tree. (Generally the DIT follows the DNS structure.)
    - *SIMS Reference Manual*, Chapter3, Directory Information Tree and Schema.
    - Chapter 4, Hosted Domains

From Installation to Going On-line

These tasks are performed after SIMS is installed on your machines.

Initial Configuration

These are tasks for configuring your system for pilot test. The pilot set up should consist of a subset of your SIMS system.

- Configure and connect your servers. This includes proxy servers, Message Stores servers, SMTP internal and internet relays, Delegated Administrator servers, regular SIMS servers, LDAP servers, DNS servers, and so on.
    - Chapter 5, Internet Message Transport Agent (IMTA) Administration
    - Chapter 6, IMTA Security and Unsolicited Bulk Email (UBE) Handling

  - Chapter 7, Message Store Administration.
  - Appendix A, Configuring SIMS as a Proxy Message Access Server.
  - *SIMS Reference Manual*.
- Setup directory service configuration. Configure directory information tree. Set masters and replicas.
  - *SIMS Reference Manual*, Chapter3, Directory Information Tree and Schema.
  - Chapter 4, Hosted Domains.
  - *SIMS Provisioning Guide*.
  - Sun Directory Services documentation (http://docs.sun.com:80/ab2/coll.297.1/@Ab2CollToc?subject=sysadmin).
  - Netscape Directory Services documentation (http://home.netscape.com/eng/server/directory/).
- Test pilot setup.

Full Configuration

These tasks are for configuring your system prior to going on-line. This setup should be as close to your on-line setup as possible.

- Configure and create IMTA channels as necessary.
  - *SIMS Reference Manual*, Chapter 2, IMTA Configuration.
  - Chapter 5, Internet Message Transport Agent (IMTA) Administration.
  - Chapter 6, IMTA Security and Unsolicited Bulk Email (UBE) Handling.
- Set user quotas.
  - "Message Store Quotas" on page 162.
- Set up SSL and Certificate Authority program.
  - "Secure Sockets Layer (SSL) Support in SIMS" on page 215.
- Configure security and unsolicited bulk email (UBE) handling.
  - Chapter 6, IMTA Security and Unsolicited Bulk Email (UBE) Handling.
  - Chapter 5, Internet Message Transport Agent (IMTA) Administration.
- Test full configuration setup.

Preparing for Deployment

For documentation references see "Defining SIMS Operational Processes and Procedures" on page 1.

- Migrate and install users and groups.
- Migrate mailboxes.

Going Live

- Instruct users about any procedural and configuration changes they need to make due to SIMS installation.
  - Do the clients need to point to a new POP/IMAP server?
  - Do users need to enter +domainname along with their login uid?
- Instruct users on how to change passwords and set vacation messages. Instruct delegated administrator on how to add and delete users.
  - *SIMS Delegated Management Guide*.

Ongoing SIMS Administration

Most of these are tasks were planned in “Defining SIMS Operational Processes and Procedures” on page 1. See the documentation references in this section.

- Adding, modifying, and removing users and groups.
- Adding, modifying, and removing hosted domains.
- Message purge and folder check schedule.
  - “Message Purge” on page 172.
- Message store backup schedule.
- Monitoring policy and procedures.
- Setup directory backup schedule.
- “SIMS Periodic Maintenance Procedures” on page 231.
- “SIMS Troubleshooting” on page 269.

SIMS Quick Task and Reference List

- TABLE 1-1, “SIMS Admin Console Task List” on page 5
- TABLE 1-2, “User Manager Tasks” on page 6
- TABLE 1-3, “Hosted Domain Tasks” on page 6
- TABLE 1-4, “General IMTA Tasks” on page 7
- TABLE 1-5, “IMTA Channel Tasks” on page 8
- TABLE 1-6, “IMTA Security and Unsolicited Bulk Email (UBE) Handling Tasks” on page 9

- TABLE 1-7, “General Message Store / Message Access Tasks” on page 10
- TABLE 1-8, “Directory Service Tasks” on page 11
- TABLE 1-9, “Populating SIMS with Users and Mailboxes” on page 12
- TABLE 1-10, “SIMS Monitoring and Logging Tasks” on page 12
- TABLE 1-11, “Unclassified SIMS Topics and Tasks” on page 12

TABLE 1-1 SIMS Admin Console Task List

Task	CLI/GUI/Configuration File Parameter Interface	Page
To Start the SIMS Admin Console	On Netscape 4.06 or greater. `http://<machine-name>/sims/` Note: Must modify `.preferences` file.	15
Creating SIMS Administrators	`imadmin-add-admin`	19
Viewing SIMS Administrators	`imadmin-search-admin`	20
Removing SIMS Administrator Privileges	`imadmin-remove-admin`	20
To Stop SIMS Components	`/etc/init.d/im.server stop` AdminConsole>SIMS Console>Stop all	21
To Start SIMS Components	`/etc/init.d/im.server start` AdminConsole>SIMS Console>Start all	21
To Log Out of the Administration Console	AdminConsole>SIMS Console>Logout	21
To Access SIMS Version Information	AdminConsole>SIMS Console>About SIMS	22
Troubleshooting the Admin Console	See the full text.	270
Troubleshooting the Administration Server	See the full text.	271

TABLE 1-2 User Manager Tasks[1]

Topic/Task	Description	Page
To Create a User Entry	`imadmin-add-user` AdminConsole>User Manager>Select Domain>Create pulldown>User	28
To Create a Group Entry	`imadmin-add-group` AdminConsole>User Manager>Create pulldown>Group	33
View a Domain	AdminConsole>User Manager>Choose Domain to Browse	38
To Find and View User/Group Entries	`imadmin-search-user/group` AdminConsole>User Manager>Highlight People or Groups>Find	38
To Delete a User or Group Entry from the Directory	`imadmin-delete-user/group`, `imadmin-purge-user/group` AdminConsole>User Manager>Highlight user>Selected Delete	41
To Modify a User Entry	`imadmin-modify-user` AdminConsole>User Manager>Display & double click the user entry	41
To Modify a Group Entry	`imadmin-modify-group` AdminConsole>User Manager>Display & double click Group Entry	49

[1] See also the SIMS Provisioning Guide.

TABLE 1-3 Hosted Domain Tasks[1]

Topic/Task	Description	Page
Mail Client Login to Hosted Domains	Default domain: uid Non-default domain: uid+domain	62
Changing the Default Separator	See the full text.	62
Allowing Users in Subdomains to Log In Using the Domain Name	See the full text.	62
To Create an Hosted Domain	`imadmin-create-domain` AdminConsole>User Manager>Create pulldown>Domain	64
To Create Hosted Domain Alias	`imadmin-add-alias`, `imadmin-delete-alias` & `imadmin-modify-alias`	66
To Delete a Hosted Domain	`imadmin-delete-domain` & `imadmin-purge-domain` AdminConsole>User Manager>Selected domain >Selected-Delete	66
Modifying a Hosted Domain	See the full text.	67

TABLE 1-3 Hosted Domain Tasks[1] *(Continued)*

Topic/Task	Description	Page
To Set Up the System So that Users Can Log in Without Entering their Domain Name	See the full text.	67
Creating Delegated Administrators	Create a user then use `imadmin-add-admin`	71
Viewing Delegated Administrators	`imadmin-search-admin`	72
Removing Delegated Administrator Privileges	`imadmin-remove-admin`	72
Creating Domain Postmaster Mailboxes	See the full text.	72
Delegated Management Console Customization	See the full text.	73

[1] See also the SIMS Provisioning Guide.

TABLE 1-4 General IMTA Tasks

Topic/Task	Description	Page
To Stop And Start the IMTA	`imta-start & imta-stop` AdminConsole>IMTA>IMTA pulldown>Start IMTA	83

To Restart the IMTA	`imta-restart`
	`AdminConsole>IMTA>IMTA pulldown>Restart IMTA`
		84

To BackUp and Restore the IMTA Configuration	AdminConsole>IMTA>IMTA pulldown>Save Current Config AdminConsole>IMTA>IMTA pulldown>Restore Def/Backup Config	84
To Monitor Channel Status	AdminConsole>IMTA>Channels	85
To Make Delivery Programs Available to Users	`imta-program`	86
To Reconfigure the Alias Synchronization Schedule	`imta-dirsync` AdminConsole>IMTA>Full/Incremental Alias Synchronization	89
To Disable Full and Incremental Synchronization	AdminConsole>IMTA>Full/Incremental Alias Synchronization>Inactive	90
To Configure IMTA Position Relative to the Internet	AdminConsole>IMTA>Position Vs. Internet	91
To Configure Routability Scope	AdminConsole>IMTA>Routability Scope	93

TABLE 1-4 General IMTA Tasks *(Continued)*

Topic/Task	Description	Page
Maintenance: Adjusting Post Job Frequency	See the full text.	232
Maintenance: Adjusting the Frequency of the Return Old Messages Program	See the full text.	232
Troubleshooting the IMTA	See the full text.	278

TABLE 1-5 IMTA Channel Tasks

Topic/Task	Description	Page
To Create a Channel	AdminConsole>IMTA>Create pulldown>Channel	96
To Delete a Channel	AdminConsole>IMTA>Channels>Selected pulldown>Delete Channel	97
To Access a Channel's Property Book	AdminConsole>IMTA>Channels	97
To Configure a Channel Description	AdminConsole>IMTA>Channels>desired channel description>Selected Menu>Properties	98
To Configure Routability Scope	AdminConsole>IMTA>Channels>selected channel>Selected Menu>Properties>Router	93
To Configure a Router Host	`imta-dirsync` AdminConsole>IMTA>Full / Incremental Alias Synchronization	99
To Configure Character Set Labels	AdminConsole>IMTA>Channels>selected channel>Selected Menu>Properties	100
To Configure Message Limitation	`imadmin-modify-msglimits & imadmin-search-msglimits` AdminConsole>IMTA>Channels>selected channel>Selected Menu>Properties>Message Limitation	101
To Configure Delivery Status Notification	`imadmin-modify-notary` & `imadmin-search-notary` AdminConsole>IMTA>Channels>selected channel>Selected Menu>Properties>Delivery Status Notification	102
To Change the Notary Message Locale	See the full text.	103
To Configure Report Failures to the Postmaster	`imadmin-modify-postmaster` & `imadmin-search-postmaster` AdminConsole>IMTA>Channels>selected channel>Selected Menu>Properties>Report Problems to Postmaster	104
To Configure Diagnostics Output	AdminConsole>IMTA>Channels>selected channel>Selected Menu>Properties>Diagnostics Output	105

TABLE 1-5 IMTA Channel Tasks *(Continued)*

Topic/Task	Description	Page
To Set Recipient Limitation	AdminConsole>IMTA>Channels>double-click channel>Properties>Performance Tuning	106
To Configure Message Logging	AdminConsole>IMTA>Channels>double-click channel>Properties>Logging	107
To Enable Reassembly of Message Fragments	AdminConsole>IMTA>Channels>double-click channel>Properties>MIME Fragmentation	109
To Add, Delete, or Modify a Rewrite Rule	AdminConsole>IMTA>Channels>double-click channel>Properties>Rewrite Rules	110
Monitoring Channel Queues	Utilities: `imta-counters`, `immonitor-queue`, SMTP command: `xstra`	112
To Monitor the IMTA Channel Queues on Admin Console	AdminConsole>IMTA>Channels>select channel>Selected pulldown>Monitor Queue	113
To Monitor the IMTA Channel Queues Using xsta	SMTP command: `xsta`	115
To View Messages Stored In the IMTA Channel Queues	AdminConsole>IMTA>Channels>selected channel>Selected Menu>Monitor Queue>Show Stored Message	116
DNS-based Canonicalization	See the full text.	118

TABLE 1-6 IMTA Security and Unsolicited Bulk Email (UBE) Handling Tasks

Topic/Task	Description	Page
Secure Sockets Layer (SSL) Support in SIMS	See the full text.	215
SMTP AUTH Configuration	See the full text.	140
SMTP Access Restrictions by IP Address and Port Number	See the full text.	124
SMTP Access Restrictions by Source and Destination Email Address	See the full text.	125
SMTP Access Restrictions by IP Address, Port, and Email Address	See the full text.	127
Limiting the Number of Recipients Per Message or the Number of Messages Per Session	See the full text.	127
DNS-based Email Access Control	See the full text.	128
Access and Relay Restrictions with the Admin Console	See the full text.	131
Optimizing Access and Relay Restrictions	See the full text.	138
Identifying the Source of Incoming SMTP Messages	See the full text.	143
Logging Messages Passing Through IMTA	See the full text.	143

TABLE 1-6 IMTA Security and Unsolicited Bulk Email (UBE) Handling Tasks *(Continued)*

Topic/Task	Description	Page
Snapshot of Message Traffic Through IMTA	See the full text.	144
Imposing Message Size Limits	See the full text.	145
Message Priority Limits	See the full text.	145
Imposing Message Sensitivity Limits	See the full text.	145
Checking or Filtering Message Content	See the full text.	146
Separating External and Internal Message Traffic	See the full text.	147
Restricting SMTP Probe Commands	See the full text.	150
Removing Internal Names in Received Headers	See the full text.	151

TABLE 1-7 General Message Store / Message Access Tasks

Topic/Task	Description	Page
Enabling APOP	`apop`	157
Enabling POP Before SMTP	`popb4smtp`	157
Message Store Support for Failover LDAP Hosts	See the full text.	157
To Back Up and Restore the Sun Message Store Configuration	AdminConsole>Sun Message Store Pulldown>Backup config	159
To Monitor Mail Store Space Usage and Settings	AdminConsole>Sun Message Store>General Options>Message Store Space Usage	160
To View Sun Message Store Paths	AdminConsole>Sun Message Store>General Options> Store Paths	161
Message Store Quotas	AdminConsole>User Manager>Dsiplay then double click the user entry>Mail Information	162
To Activate Message Store Quota Enforcement on an Installed System	See the full text.	163
To Set a User's Mail Store Quota	AdminConsole>User Manager>Display & double click the user entry	164
To Monitor User Quotas	`imquotacheck -v`	165
To Warn Users When Their Mail Store Usage Is Approaching Their Mail Store Quota	`imquotacheck -f`	166
Setting Soft Quotas	See the full text.	167
To Configure Advanced Options	AdminConsole>Sun Message Store>Advanced Options	170

TABLE 1-7 General Message Store/Message Access Tasks *(Continued)*

Topic/Task	Description	Page
To Configure Purge Options	AdminConsole>Sun Message Store>Purge Options	174
To Configure the Purge Schedule	AdminConsole>Sun Message Store>Schedule For Purging Deleted Messages	175
Message Access Protocol Connections	AdminConsole>Message Access	176
Sun Message Store Maintenance	See the full text.	234
Message Store Backup and Restore	`imbackup` & `imrestore` See the full text.	237
Message Store Data Check	`imcheck`	244
Importing /var/mail Users	`imimportmbox` (see also “Migrating Mailboxes from /var/mail to SIMS” on page 315)	245
Deleting Old Messages	`imexpire`	245
To Disable Automatic Quota Synchronization	See the full text.	246
Deleting the User	`imadmin-delete-user`	246
Troubleshooting the Message Store	See the full text.	274

TABLE 1-8 Directory Service Tasks

Topic/Task	Description	Page
Sun Directory Services documentation	http://docs.sun.com:80/ab2/coll.297.1/@Ab2CollToc?subject=sysadmin	
Netscape Directory Services documentation	http://home.netscape.com/eng/server/directory/	
Specifying Current and Backup LDAP Servers for SIMS	`imadmin-modify-currentldap` & `imadmin-add-ldapserver`	180

Starting and Stopping the Sun Directory Services	`# /etc/init.d/dsservd start`
	`# /etc/init.d/dsservd restart`
	`# /etc/init.d/dsservd stop`
		181

Viewing Sun Directory Services Configuration for SIMS	See the full text.	182
Troubleshooting the Directory Service	See the full text.	295

TABLE 1-9 Populating SIMS with Users and Mailboxes

Topic/Task	Description	Page
Populating the Directory	*SIMS Provisioning Guide*	
Populating the Directory from NIS, NIS+, or /etc Files Entries	See the full text.	190
Populating the Directory with User Data—Sample Session	See the full text.	321
Populating the Directory with User Aliases Data and Distribution Lists —Sample Session	See the full text.	325
Migrating Mailboxes from /var/mail to SIMS	See the full text.	315

TABLE 1-10 SIMS Monitoring and Logging Tasks

Topic/Task	Description	Page
Logging Facilities	See the full text.	250
Message Store/Message Access Log Files	Log messages in `/var/log/syslog` and prefixed with `SUNWmail.ims`	250
Sun Directory Service Log Files	`/var/opt/SUNWconn/ldap/log`	251
IMTA Log Files	`/var/opt/SUNWmail/imta/log`	252
Identifying the Source of Incoming SMTP Messages	See the full text.	254
Logging Messages Passing Through the IMTA	See the full text.	254
Snapshots of Message Traffic through the IMTA	`imta-counters` (See the full text.)	257
SIMS Monitoring Plan	See the full text.	261

TABLE 1-11 Unclassified SIMS Topics and Tasks

Topic/Task	Description	Page
Crash Recovery	See the full text.	297
Configuring SIMS as a Proxy Message Access Server	See the full text.	301

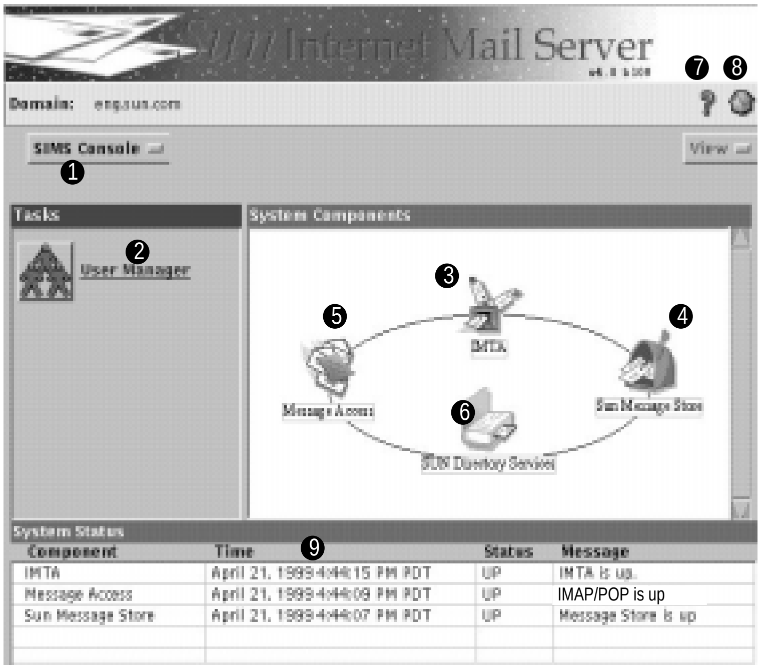
CHAPTER **2**

The SIMS Administration Console Overview

The *Admin Console* provides a browser-based GUI interface for common SIMS administrative tasks, namely SIMS configuration, and populating the system with users and groups. Note that only one administrator can be logged on to the Admin Console at a time. The first screen of the Admin Console is shown below.

Tasks:

1. Logout, Stop SIMS
2. Create/Modify User, Group or Domain
3. Configure message transport agent/ Monitor Queued Messages
4. Configure/Monitor Message Storage attributes
5. View all client message access connections to SIMS
6. Bring up the Sun Directory (LDAP) Services Admin Console
7. Help
8. Home
9. View SIMS Component Status



Component	Time	Status	Message
IMTA	April 21, 1999 4:44:15 PM PDT	UP	IMTA is up.
Message Access	April 21, 1999 4:44:09 PM PDT	UP	IMAP/POP is up
Sun Message Store	April 21, 1999 4:44:07 PM PDT	UP	Message Store is up

FIGURE 2-1 Admin Console Home Page

TABLE 2-1 SIMS Admin Console Home Page (see FIGURE 2-1 on page 13)

Components/Task	Description	Page
1) Stopping SIMS, Logging Out, and Version Information	Self Explanatory	21
2) User/Group Management	Provides instructions for adding, deleting, or modifying user, group or organizational units entries in the directory.	23
3) Message Store Administration	Monitor and customize the SIMS message storage and access characteristics by modifying the parameters of this component. The Message Store chapter provides instructions for monitoring message store paths, space usage and user space quotas; configuring user quotas, mail server client type, maximum connections, disk space threshold, `/var/mail` support, message store size increase, and message purge schedule.	155
4) Internet Message Transport Agent (IMTA) Administration	The IMTA receives, routes, and sends incoming messages to their destination. SIMS message transport can be customized by modifying the IMTA attributes. This chapter provides instructions for viewing and changing the message transport characteristics of SIMS, including configuring/monitoring channels, directory cache update, anti-spam features, IMTA location relative to the Internet, and routability scope.	81
5) Message Access Protocol Connections	View and monitor all user connections to SIMS, as well as start and stop client access to the message store.	176
6) Sun Directory Services Administration	The Directory Service contains the routing information for SIMS. Pressing this icon brings up the Sun Directory Service log on screen. If the Netscape Directory Server is installed, this icon will not appear. For complete information refer to the Sun Directory Service or Netscape Directory Service documentation.	179
7) Help	Online help for SIMS.	
8) Home	Return to Home Page.	
9) SIMS Component Status	Display the current state of each component.	17

Admin Console Tips and Information

- Not all tasks can be done on the Admin Console. Some tasks require editing SIMS configuration files, others require running UNIX commands, and still others require using the directory service interface. Wherever possible, we try to state which these permissions, accounts, or interface is needed to perform a specific SIMS task.
- Most Admin Console tasks can be accomplished by using one or more *other* methods. These methods include:

- Modifying a configuration file.
- Executing a SIMS utility or command.
- Modifying the LDAP directory.

When a command can perform the same task as the Admin Console, that command is listed under the title of a task section. (Note that multi-word commands are listed with hyphens between them for example `imadmin-add-user`. The actual command requires spaces in place of the hyphens, however, to bring up the man page you need to include the hyphens.) See the man page for more details. Information on SIMS configuration files can be found in the *SIMS Reference Manual* or in a man page.

- Generally using the Admin Console is not as fast as using the command line interfaces or modifying the LDAP directory directly. However it's usually easier and provides a bit of protection by asking for confirmations, as well as not modifying restricted lines or parameters.
- When you set a configuration in the Admin Console, press the Apply button to save your settings. If you don't do this, you may lose your settings if you exit the page on which you specified your configurations.
- The same login and password required to log on to the Admin Console can be used to execute the `imadmin` provisioning utilities. See the `imadmin` man page for details.

▼ To Start the SIMS Admin Console

You must use the Netscape 4.05 browser and above for the Admin Console to work properly. If you are using the Netscape browser, you **MUST** add the following line in`.netscape/preferences.js` (Solaris Operating Environment) or in `user/<username>/pref.js` (Windows NT) for the Admin Console to run correctly:

```
user_pref("signed.applets.codebase_principal_support",true);
```

Failure to set this arguments could cause deleterious effects on your system.

To bring up the Admin Console, start the browser and go to `http://<machine-name>/sims/`. Enter the SIMS administrator's login (default: `siteadmin`), the domain to which the administrator belongs, (specified at installation) and the password.

Note – If you are running on the Netscape browser, you need to run the browser as a regular user on the Solaris and Windows NT desktop. Running as a super user on the desktop does not have the setup to run Java applets.

Admin Console Topics and Tasks

TABLE 2-2 Admin Console Topics and Tasks

Topic/Task	Description	Page
Admin Console Buttons	Describes buttons that appear in the Admin Console	16
SIMS Component Status	Describes component status flags on Admin Console Home page	17
Creating and Removing SIMS Administrators	How to create, remove, modify SIMS administrator privileges and passwords.	18
Stopping SIMS, Logging Out, and Version Information	Starting/stopping SIMS components, logging out of the SIMS Admin Console, accessing SIMS versioning information.	21

Admin Console Buttons

TABLE 2-3 describes the most common buttons that appear in the Admin Console or dialog boxes.

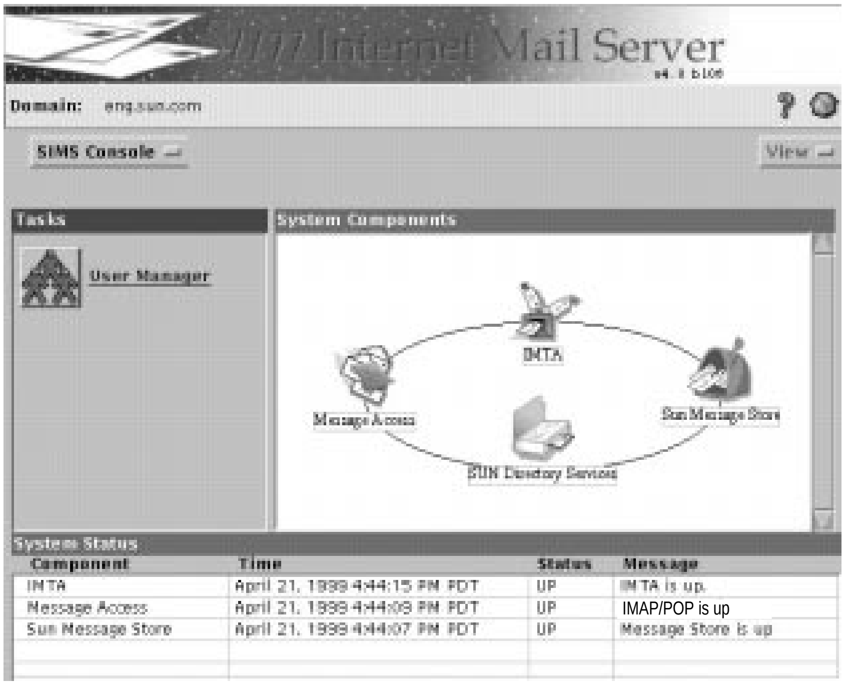
TABLE 2-3 Buttons and Associated Actions

Button	Explanation
Apply	Submits the changes made to the configuration file associated with the current page. If the changes made require a restart of the associated component, a dialog box prompts you to restart the component. The current page remains displayed.
Cancel	Discards the changes made to the configuration file associated with the current page. The previous page displays.
Help icon or button	Displays documentation specific to the Admin Console page or dialog that you are attempting to configure.
OK	Submits the changes made to the configuration file associated with the current page. If the changes made require a restart of the associated component, a dialog box prompts you to restart the component. The previous page displays.
Reset	Discards the changes made to the configuration file associated with the current page and sets the values of the changed attributes to their last saved value. The current page remains displayed.

Tip – When you set a configuration, you must press the Apply button to save your settings. If you do not do this, you may lose your settings. You are not always warned about losing the settings when you exit a page.

SIMS Component Status

SIMS polls each component (except the directory service) periodically to determine its current state. The System Components on the Admin Console home page (FIGURE 2-2) displays the current state of each component. TABLE 2-4 outlines the possible SIMS component states.



Component	Time	Status	Message
IMTA	April 21, 1999 4:44:15 PM PDT	UP	IMTA is up.
Message Access	April 21, 1999 4:44:09 PM PDT	UP	IMAP/POP is up
Sun Message Store	April 21, 1999 4:44:07 PM PDT	UP	Message Store is up

FIGURE 2-2 Monitoring Current Component State

TABLE 2-4 SIMS Component States

Component State	Icon Representation	Explanation
Up	Component icon.	Component is functioning normally.
Alert	Component icon with exclamation point overlaid.	Component has a nonfatal problem and is still functioning.
Down	Component icon with cross-bars overlaid.	Component has a fatal problem and is not functioning.

If a System Component graphic indicates that a component is in either an alert or down state, you can access more information from the System Status section on the Admin Console home page. Each entry indicates the time at which the component was polled, the component status, and more detailed information about if the component is in either an alert or down state.

If the Internet Message Transfer Agent (IMTA) is in an alert or down state, you should also check the status of each IMTA channel. For more information, refer to "Monitoring Channel Status" on page 85.

For more problem resolving information see **Chapter 13, "SIMS Troubleshooting**."

Note – The *Stop all* function on the home page does not stop the Directory Service so the Directory Services icon will not have a red X over it if you execute this procedure (see "To Stop SIMS Components" on page 21).

Creating and Removing SIMS Administrators

SIMS requires a variety of different permissions and accounts to access and service all the SIMS administrative capabilities. For example:

- To log on to the SIMS Admin Console, and to be able to execute the `imadmin` commands (example: `imadmin-add-user`) requires a SIMS administrator login and password.
- To execute IMTA and message store configuration commands, as well as message store maintenance functions, the inetmail UNIX account is required.

- To modify the Sun Directory Services configuration and to create replicas, the Sun Directory Services or NetScape Directory Services login and password are required. which are different from their SIMS login and password.

A default SIMS administrator is created at installation called *siteadmin*. In this document, a SIMS administrator refers to a user who has the ability to log on to the SIMS Admin Console and to execute the `imadmin` commands.

Wherever possible, we try to state these permissions and accounts needed to perform a specific task.

▼ Creating SIMS Administrators

Utilities: `imadmin-add-admin`, `imadmin-search-admin`, `imadmin-remove-admin`

SIMS administrators can log on to the SIMS Admin Console and can also execute the `imadmin` commands. A *SIMS administrator* is different from a *delegated administrator* who can only add, modify, delete, and search for group or user entries at a specified hosted domain. A SIMS administrator can modify any entries in any part of the directory and can configure any part of the entire SIMS system.

A SIMS administrator is created by another SIMS administrator using the utility `imadmin-add-admin` and by setting the appropriate ACLs for the entry. These ACLs are `write` permission for the `userPassword` attribute for all users, and `write` permission for the sub-tree beneath `o=internet`. For example, in the Sun Directory Service you might add the following to `/etc/opt/SUNWconn/ldap/current/dsserv.acl.conf`

```
access to
attrs=mailAutoReplyStartDate,mailAutoReplyExpirationDate,mailAutoRe
plyTimeout,mailAutoReplySubject,mailAutoReplyText,mailAutoReplyText
Internal,mailDeliveryOption,mailForwardingAddress,mailProgramDelive
ryInfo,userDefinedAttribute1,userDefinedAttribute2,userDefinedAttri
bute3,userDefinedAttribute4,mail,rfc822MailAlias,description,seeAls
o,telephoneNumber,facsimileTelephoneNumber,l,ou,physicalDeliveryOff
iceName,postOfficeBox,postalAddress,postalCode,preferredDeliveryMet
hod,registeredAddress,st,street,telephoneNumber,title,carLicense,gi
venName,homePhone,homePostalAddress,initials,jpegPhoto,labeledURI,m
obile,pager,roomNumber
    by self write
    by dn="cn=<Admin>,ou=People,dc=bridge,dc=net,o=internet" write

access to attrs=userPassword
    by self write
    by dn="cn=<Admin>,ou=People,dc=bridge,dc=net,o=internet” write
    by * compare
```

```
access to dn=".*o=internet"
    by dn="cn=<Admin>,ou=People,dc=bridge,dc=net,o=internet" write
```

If the Netscape Directory Service is installed and *configured by SIMS during the installation process*, imadmin-add-admin will complete the admin creation process. If the Netscape Directory Service is installed, but *not configured by SIMS during installation*, then you must set the appropriate permissions for the new administrator entry. This involves setting the appropriate access control items (ACIs). See the Netscape Directory Service documentation for further information.

Note – imadmin-add-admin allows you to create both delegated administrators and SIMS administrators. To create a SIMS administrator, do not specify a domain in the argument list or you will create a delegated administrator. delegated administrators have fewer administrative capabilities. See “Creating, Viewing and Removing Delegated Administrators and Postmasters” on page 71.

▼ Changing the SIMS Administrator Password

Use the imadmin-modify-user utility to modify the userPassword attribute of a SIMS Administrator. Note that you cannot change the password of the SIMS “super” Administrator through the Admin Console or Delegated Management Console (the SIMS administrator as defined by the adminBindDN attribute in the /etc/opt/SUNWmail/sims.cnf file). If you forget the SIMS “super” Administrator password, contact your Sun Microsystems support person.

▼ Viewing SIMS Administrators

A list of users who have SIMS administrator or delegated administrator privileges for a particular domain can be generated with the utility imadmin-search-admin

▼ Removing SIMS Administrator Privileges

SIMS administrator privileges can be removed by a SIMS administrator using the utility imadmin-remove-admin.

Stopping SIMS, Logging Out, and Version Information

This section describes tasks that affect the Admin Console. They are:

- "To Stop SIMS Components" on page 21
- "To Log Out of the Administration Console" on page 21
- "To Access SIMS Version Information" on page 22

▼ To Stop SIMS Components

Utility: `/etc/init.d/im.server stop`

To stop the SIMS components (IMTA, Sun Message Store, and message access protocols), go to the Admin Console Home Page, click on the SIMS Console menu and select *Stop all*.

▼ To Start SIMS Components

Utility: `/etc/init.d/im.server start`

To start the SIMS components (IMTA, Sun Message Store, and message access protocols), if they are not already started, go to the Admin Console Home Page, click on the SIMS Console pull-down menu and select *Start all*. This is only available if a component is stopped.

▼ To Log Out of the Administration Console

After you are finished with the Admin Console you may log out by going to Admin Console Home Page, clicking the SIMS Console menu, and selecting *Logout*.

Note – For security reasons, we recommend logging out of the SIMS Admin Console after a task is complete. Also, since only one administrator at a time can be logged on, remaining logged on locks other administrators out of the system.

▼ To Access SIMS Version Information

Access the SIMS Version for all SIMS components by going to the Admin Console Home Page, clicking the SIMS Console menu, and selecting About SIMS.

CHAPTER 3

User/Group Management

This chapter describes how to add, delete, or modify user and group *entries* using the SIMS Admin Console. Corresponding command-line utilities are also referenced. See the utility’s man page for complete information (imadmin utility man pages are at `/opt/SUNWmail/admin/man` or `<basedir>/opt/SUNWmail/admin/man` on an high availability installation).

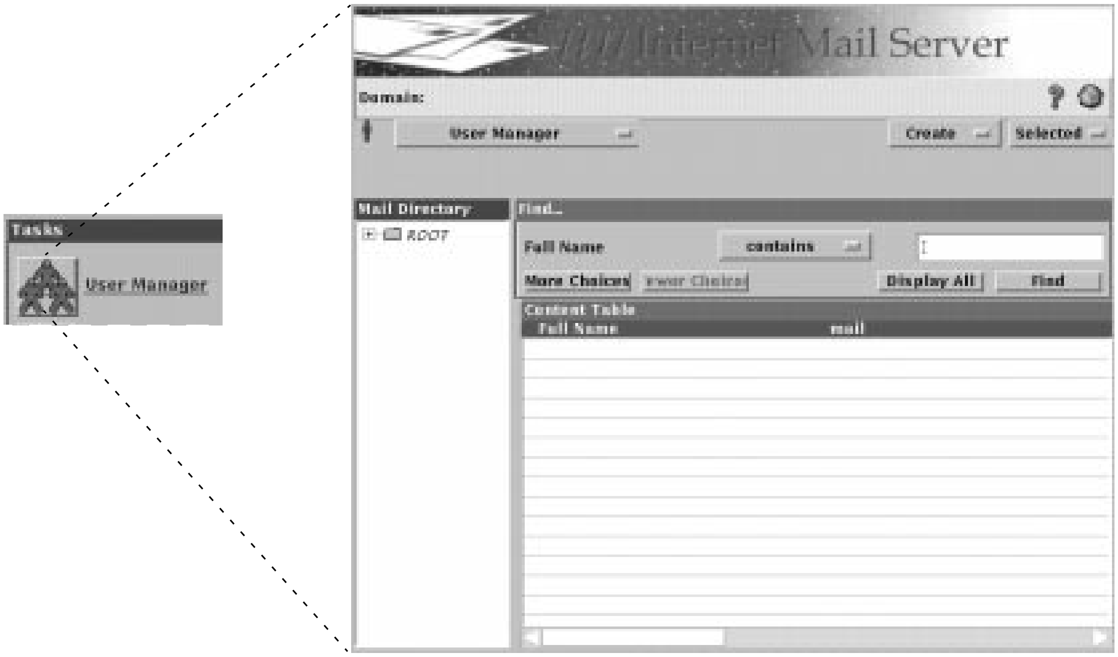


FIGURE 3-1 User Manager Page

Note – We recommend using the Admin Console or `imadmin` utilities to create, delete, and modify mail entries, however, if you have modified the SIMS schema you may need to use the directory service commands `ldapadd`, `ldapmodify` and `ldapdelete` instead. For Refer to the man pages in `/opt/SUNWconn/man`.

User Management Topics and Tasks

TABLE 3-1 User Manager Topics and Tasks

Topic/Task	Description	Page
To Create a User Entry	How to add a new mail/calendar user to the directory.	28
To Create a Group Entry	How to add a group entry to the directory.	33
View a Domain	View a domain in the DIT	38
To Find and View User/Group Entries	Searching for an entry and displaying its property sheet.	38
To Delete a User or Group Entry from the Directory	How to remove a user or group entry from the directory.	41
To Modify a User Entry	Changing User entries.	41
To Modify a Group Entry	Changing a group entry.	49
User Management Error Messages	Error messages that occur when doing user management.	329

User/Group Management Commands and Attributes

Email users and groups are defined my entries in the SIMS directory server. Routing and personal information about groups and users are specified by assigning values to the desired SIMS LDAP attributes. This can be done directly by modifying a user or group’s LDAP entry (see the *SIMS Provisioning Guide*), by using the `imadmin` provisioning utilities (see the `imadmin` man page), or by using the Admin Console. This chapter focuses primarily on the Admin Console.

TABLE 3-2 User and Group Management Commands

imadmin-add-user	imadmin-add-group
imadmin-modify-user	imadmin-modify-group
imadmin-delete-user	imadmin-delete-group
imadmin-search-user	imadmin-modify-group

TABLE 3-3 User Attributes/Fields

Field	Description
Personal Information/Name	
Distinguished name (dn)	(Required.) A unique path name associated with a user entry that reflects the hierarchy of the directory information tree.
Full name	(Required.) Stores the possible variations of the first name, last name, and middle initial fields combined. The middle initial is optional. Examples of full names for one particular user are Harrison Green, Harry Green, and Harry A. Green.
First Name	(Not required.) For example, in the case of Harry Green, the first name is Harry.
Last Name	(Required.) A last name is a surname, for example, in the case of Harry Green, the last name is Green.
Middle Initial	(Not required.) The middle initial is the first letter of the middle name, for example, in the case of Harry A. Green, the initial is A.
Title	(Not required.) A business or personal title, for example, Accountant or Avid Science Fiction Fan, respectively.
Personal Information/Telephone	
Telephone Number	(Not required.) Can also include extension number.
Fax Number	(Not required.) Self explanatory.
Pager Number	(Not required.) Self explanatory.
Mobile Phone Number	(Not required.) Self explanatory.
Personal Information/Address	
Postal address	(Not required.) Self explanatory.
Location	(Not required.) Self explanatory.
Office Number	(Not required.) Self explanatory.

TABLE 3-3 User Attributes/Fields *(Continued)*

Field	Description
Personal Information/Miscellaneous	
Home Page	(Not required.) The Uniform Resource Locator (URL) for a home page.
Description	(Not required.) Self explanatory.
Additional Information	(Not required.) Self explanatory.
System Information	
Login name	(Required.) Unique identification (ID) for user, for example, harryg.
Password	(Required.) Password associated with login name field; can be stored clear (unscrambled) or encrypted (scrambled)
Mail Information	
Email Person Status	Active of inactive.
Mail Host	(Required.) Name of the user's mail server.
Internet Mail Delivery Options	(Required.) Location of user's Inbox. Can be either `/var/mail` or the Sun Message Store. If `/var/mail`, then must specify mailbox directory. Can optionally enable auto reply, program, forward, and append to file features.
Program Delivery Info	(Required if program feature is enabled in Internet Mail Delivery Options.) Specifies one or more commands with arguments to deliver to a UNIX program.
Forwarding Address	(Required if forward feature is enabled in Internet Mail Delivery Options.) Internet address to which email should be forwarded.
Delivery File	(Required if append to file feature is enabled in Internet Mail Delivery Options.) Pathname of file to which email should be attached to the end of.
Calendar Information	
Calendar Host	(Required for Web Access calendars.) Calendar Server host name
Default Calendar	(Required for Web Access calendars.) Name of default Calendar.

TABLE 3-4 Group Attributes/Fields

Field	Required	Description
General info./General		
Distinguished name (dn)	(Required.) A unique pathname associated with a group entry that reflects the hierarchy of the directory information tree (DIT).	
Full name	(Required.) A *full name* is the possible variations of the group address. An example of a full name for one particular group is marketing.	

TABLE 3-4 Group Attributes/Fields *(Continued)*

<table>
<tr><th>Field</th><th>Required</th><th>Description</th></tr>
<tr><td>Mail domain</td><td colspan="2">(Required.) The mail domain in which a group’s mail server resides, for example, sales.alpha.com.</td></tr>
<tr><td>Send Error Conditions To</td><td colspan="2">(Required.) The individual who receives a notice when an error condition related to the distribution list arises, for example, if a message addressed to the distribution list cannot be delivered.</td></tr>
<tr><td>Send Request Messages To</td><td colspan="2">(Required.) The individual who receives a notice when another individual requests being added as a distribution list member.</td></tr>
<tr><td>Mail Host</td><td colspan="2">(Required.) The hostname of the group’s mail server.</td></tr>
<tr><td>Password</td><td colspan="2">(Required.) Password associated with group and with a shared mailbox; can be stored clear (unscrambled) or encrypted (scrambled). You are prompted for this password when attempting to modify group entry attributes using the command line interface or the user administration interface.</td></tr>
<tr><td colspan="3"><b>General info./Telephone</b></td></tr>
<tr><td>Expandable</td><td colspan="2">(Not Required.) Make list of members for a particular group or distribution list accessible to all users.</td></tr>
<tr><td>Telephone Number</td><td colspan="2">(Not Required.) Telephone number for the group. Can include extension number.</td></tr>
<tr><td>Fax Number</td><td colspan="2">(Not Required.) Fax number for the group.</td></tr>
<tr><td>Pager Number</td><td colspan="2">(Not Required.) Pager number for the group.</td></tr>
<tr><td>Mobile Phone Number</td><td colspan="2">(Not Required.) Mobile phone number for the group.</td></tr>
<tr><td colspan="3"><b>General info./Address</b></td></tr>
<tr><td>Postal address</td><td colspan="2">(Not Required.) Postal address for the group.</td></tr>
<tr><td>Location</td><td colspan="2">(Not Required.) Location for the group.</td></tr>
<tr><td>Building</td><td colspan="2">(Not Required.) Building of the group.</td></tr>
<tr><td>Office Number</td><td colspan="2">(Not Required.) Office number for the group.</td></tr>
<tr><td>Home Page</td><td colspan="2">(Not Required.) The Uniform Resource Locator (URL) for a home page.</td></tr>
<tr><td>Description</td><td colspan="2">(Not Required.) Description for the group.</td></tr>
<tr><td>Additional Information</td><td colspan="2">(Not Required.) Additional information for the group.</td></tr>
<tr><td colspan="3"><b>Owner</b></td></tr>
<tr><td>Owner</td><td colspan="2">(Required.) An owner is an individual who is responsible for a distribution list. An owner can add or delete distribution list members.</td></tr>
<tr><td colspan="3"><b>Moderator</b></td></tr>
<tr><td>Moderator</td><td colspan="2">(Not Required.) If moderator feature is enabled, a message addressed to a distribution list is initially sent to the moderator only. The moderator can take one of the following actions: forward the message to the distribution list, edit the message and then forward it, or not forward the message.</td></tr>
</table>

TABLE 3-4 Group Attributes/Fields *(Continued)*

<table>
<tr><th>Field</th><th>Required</th><th>Description</th></tr>
<tr><td colspan="3"><b>Member Information</b></td></tr>
<tr><td>Member</td><td colspan="2">A member is a user or group who receives a copy of an email addressed to a distribution list.</td></tr>
<tr><td colspan="3"><b>Additional Delivery Options</b></td></tr>
<tr><td>Shared Mailbox</td><td colspan="2">(Not Required.) Specifies that messages are delivered to a shared mailbox in the Sun Message Store.</td></tr>
<tr><td>Program</td><td colspan="2">(Not Required.) Specifies one or more commands with arguments to deliver to a UNIX program.</td></tr>
<tr><td>Append to File</td><td colspan="2">(Not Required.) Path name of file to which email should be appended (attached to the end of).</td></tr>
<tr><td colspan="3"><b>Access Control</b></td></tr>
<tr><td>Authorized Domain</td><td colspan="2">(Not Required.) Domain name from which users or groups are authorized to send messages to a particular distribution list.</td></tr>
<tr><td>Unauthorized Domain</td><td colspan="2">(Not Required.) Domain name from which users or groups are not authorized to send messages to a particular distribution list.</td></tr>
<tr><td>Authorized Submitter</td><td colspan="2">(Not Required.) Name of user or group who are authorized to send messages to a particular distribution list. If the user or group is internal to the email system, specify the distinguished name; if external to the email system, specify an email address in RFC 822 format.</td></tr>
<tr><td>Unauthorized Submitter</td><td colspan="2">(Not Required.) Name of user or group who are not authorized to send messages to a particular distribution list. If the user or group is internal to the email system, specify the distinguished name; if external to the email system, specify an email address in RFC 822 format.</td></tr>
</table>

Admin Console User Management

This section describes user management using the SIMS Admin Console.

▼ To Create a User Entry

Utility: `imadmin-add-user`

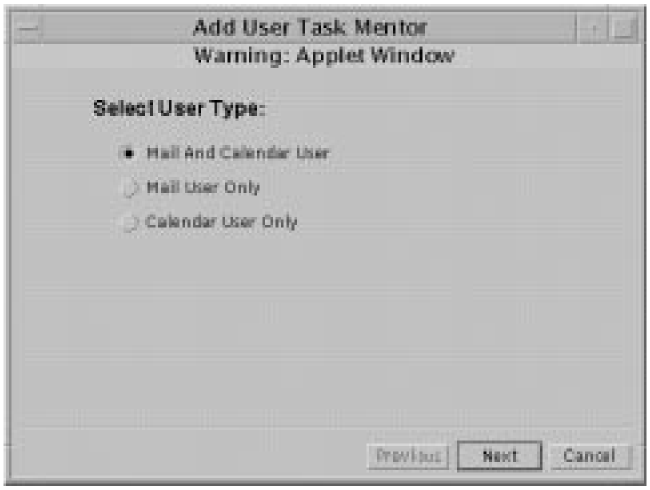
There are three kinds of users: an email and e-calendar user, an email-only user, or a e-calendar-only user. The Admin Console is useful for manually adding or modifying a small number of user entries after initial directory population. To initially populate the directory or to add a large number of user entries at one time, refer to Chapter 9, “Populating SIMS with Users and Groups or the *SIMS Provisioning Guide*.

Note – Newly created users will not receive mail until after an incremental or full `dirsync` occurs. See “To Reconfigure the Alias Synchronization Schedule” on page 89.

AdminConsole>User Manager>Select Domain in Mail Directory>Create pulldown>User

1. **In the Admin Console home page, click the User Manager icon.**
2. **Select the domain in the Mail Directory in which you wish to create the user.**

   If you are displaying the domain in which you wish to create a user, go to step 2. If it is not displayed, select User Manager>Select Choose Domain to Browse. Enter the fully qualified domain name under which the user entry will be created. For example: stream.com.
3. **Select Create>User.**
4. **Select one of the three user types as shown below and click Next.**



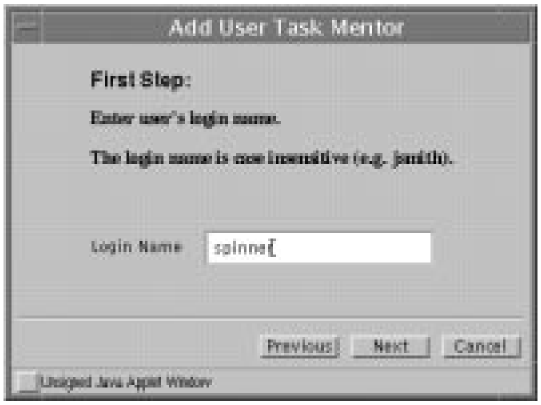
Select User Type:

● Mail And Calendar User
○ Mail User Only
○ Calendar User Only

FIGURE 3-2 Add User Task Mentor Dialog for User Type

5. Enter user's login name in First Step window and click Next

   The login name must be unique to this domain, but not necessarily the entire directory tree. That is, another domain can have the same login name. Example: `spinner@bridge.net` and `spinner@stream.com`.



Add User Task Mentor

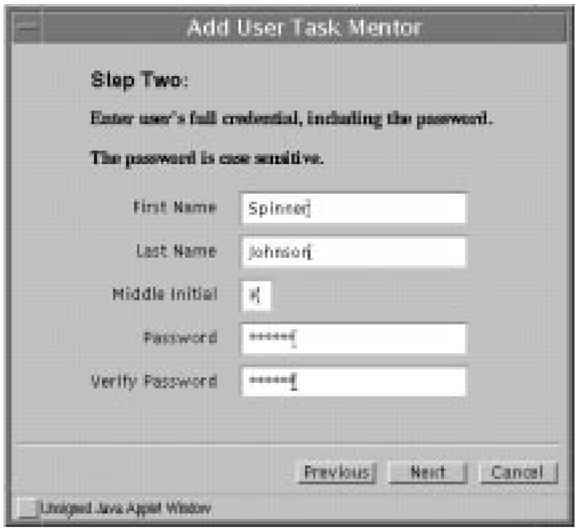
First Step:

Enter user's login name.

The login name is case insensitive (e.g. jsmith).

Login Name: spinner

6. **Enter the full name and password (password is case-sensitive) and click Next.**



Add User Task Mentor

Step Two:

Enter user's full credential, including the password.

The password is case sensitive.

First Name: Spinner

Last Name: Johnson

Middle Initial: [illegible]

Password: ******

Verify Password: ******

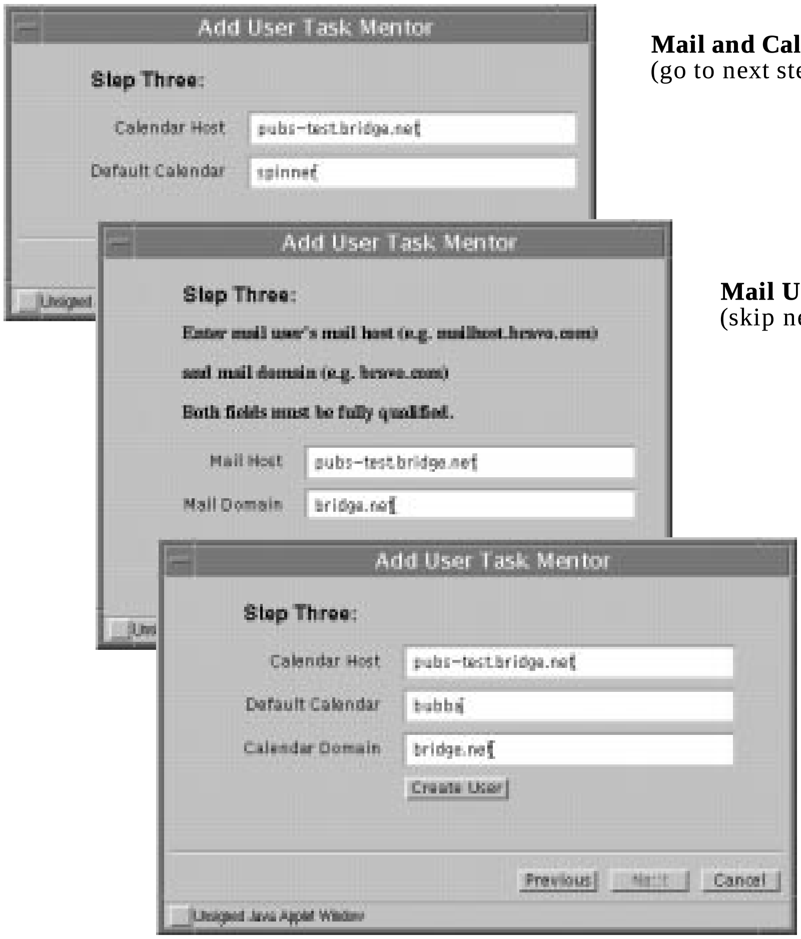
FIGURE 3-3 Add User Task Mentor Dialog for User Credentials

Note – The option you select in Step 4 determines the next dialog window to appear.

---

7. **Enter the information for the option you selected in Step 4and click Next. If you chose Calendar Use Only for Step 4, press Create User for Option 3 Calendar User Only.**

   The option you select in Step 4 determines the dialog window display as well as the next step in the process.



Add User Task Mentor

Step Three:

Calendar Host: pubs-test.bridge.net

Default Calendar: spinner

Mail and Calendar User
(go to next step)

Add User Task Mentor

Step Three:

Enter mail user's mail host (e.g. mailhost.bravo.com)

and mail domain (e.g. bravo.com)

Both fields must be fully qualified.

Mail Host: pubs-test.bridge.net

Mail Domain: bridge.net

Mail User Only
(skip next step)

Add User Task Mentor

Step Three:

Calendar Host: pubs-test.bridge.net

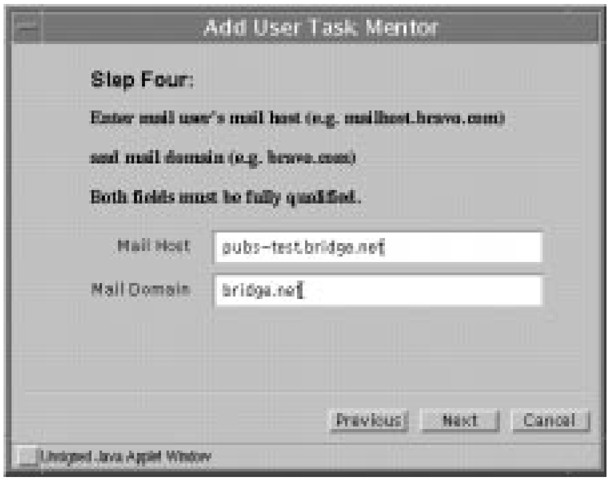
Default Calendar: bubba

Calendar Domain: bridge.net

Calendar User Only
(done—click Create User)

FIGURE 3-4 Options for Mail and Calendar, Mail Only, or Calendar Only Users.

8. **For Mail and Calendar Users, enter the Mail Host name and Mail Domain.**



Step Four:

Enter mail user's mail host (e.g. mailhost.bravo.com)

and mail domain (e.g. bravo.com)

Both fields must be fully qualified.

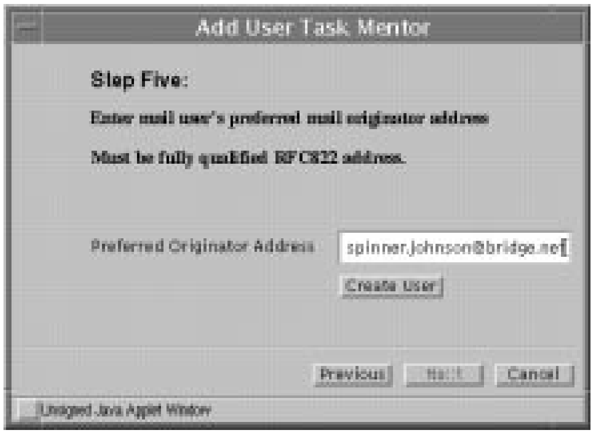
Mail Host: pubs-test.bridge.net

Mail Domain: bridge.net

FIGURE 3-5 Mail User's Host and Domain Dialog.

9. **If necessary, enter the preferred originator address for the user.**

   A preferred originator address is a mail address that a recipient outside the email system will see when a message from this user is received. If possible, the mail server detects a default preferred originator address and provides information in the appropriate fields. Review the default information for correctness. Field must be fully qualified and in RFC 822 format. The following dialog appears.



Step Five:

Enter mail user's preferred mail originator address

Must be fully qualified RFC822 address.

Preferred Originator Address: spinner.johnson@bridge.net

FIGURE 3-6 Dialog for Preferred Originator.

10. **If finished, click Create User.**

To Create a Group Entry

Utility: `imadmin-add-group`

A group entry is also known as a *distribution list*. When a message is sent to the group address, SIMS sends the message to all members in the group. You can also create a shared mailbox to which all the messages sent to the group are saved. To do this, first create a group entry (instructions below), then modify the group entry by following the instructions in “To Modify a Group Entry” on page 49, for creating the shared mailbox.

Note – The Admin Console is practical for adding small numbers of group entries. To add large numbers of group entries at one time, see Chapter 9, “Populating SIMS with Users and Groups” and the *SIMS Provisioning Guide*.

AdminConsole>User Manager>Create pulldown>Group

1. **In the Admin Console home page, click User Manager.**
2. **Select the domain in which you wish to create the group.**

   If the desired domain is not displayed, Select User Manager>Select Choose Domain to Browse. Enter the fully qualified domain name under which the user entry will be created. For example: `stream.com`. You must have a domain before you can create a group.

3. **Choose Group from the Create menu.**

   The Add Group Task Mentor dialog displays.

4. **Enter the group name, mail domain, and password. Press the Enter or Return key after entering each field.**

   The login name is case-insensitive. The mail domain must be fully qualified. For example, you could input the following for the distribution list writers:

Name:	`writers`
Mail Domain:	`bridge.net`
Password:	`******`
Verify password:	`******`

5. **Click the Next button.**
6. **Identify the owner of the distribution list.**

   The owner can add or delete distribution list members. The owner must be a user in that domain.

a. **Specify the owner's email address.**

The email address must be fully qualified. For example, to specify Chamique Campbell as the owner of the distribution list, enter the following email address:

```
chamique.campbell@bridge.net
```

b. **Click the Next button.**

The next Add Group Task Mentor dialog appears.

7. **Do you want the distribution list to be moderated?**

A moderator is member of the group—usually the owner of the distribution list—who initially receives a message addressed to a distribution list. Upon receipt of a message, the moderator can forward the message to the distribution list, edit the message then forward it to the distribution list, or not forward the message to the distribution list. During creation you can only designate one moderator, however, you can add additional moderators by modifying the group entry ("To Modify a Group Entry" on page 49)

a. **Click the Yes radio button if you want the distribution list to be moderated. Click No if you do not want the distribution list to be moderated.**

b. **If you decided to have the distribution list moderated, specify the moderator's email address.**

The email address must be fully qualified, though it can be outside of the email domain. For example, to specify Bernie Miller as the moderator of the distribution list, enter the following email address:

```
bernie.miller@bridge.net
```

c. **Click the Next button.**

8. **Do you want the group members viewable by the <expn> command?**

a. **Click the Yes radio button if you want the distribution list members to be viewable by all users in the email system. Click the No radio button if not.**

b. **If you clicked the Yes button, you must set up a mail host through which the distribution list members can be viewed.**

Enter a fully qualified mail host name. For example, to designate `mailhost1` in the `bridge.net` domain as the mail host through which the members can be viewed, enter the following:

```
mailhost.bridge.net
```

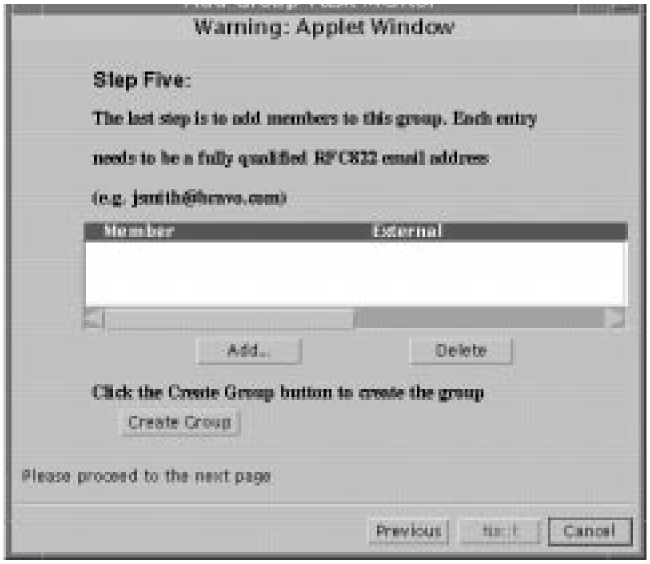
Users in the email system can view the list of members by establishing a telnet session with the specified mail host, specifying port 25, and using the following syntax:

```
expn <distribution-list-name>
```

For example, to view the distribution list of `writers`, enter the following command:

```
expn writers
```

c. **Click the Next button and add or delete distribution list members.**



Warning: Applet Window

Step Five:

The last step is to add members to this group. Each entry needs to be a fully qualified RFC822 email address (e.g. jsmith@bravo.com)

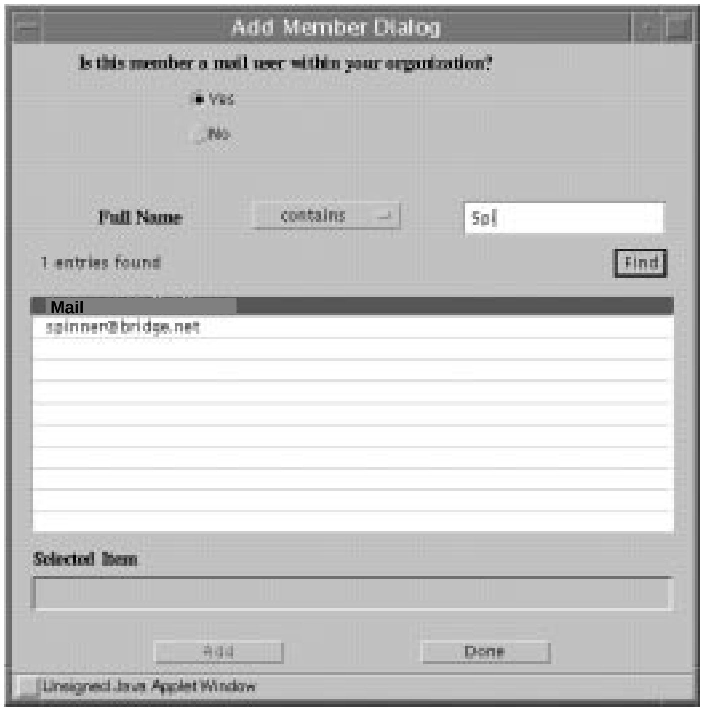
Click the Create Group button to create the group

Please proceed to the next page

FIGURE 3-7 Add Group Task Mentor Dialog

d. Add members by clicking the Add button.

The Add Member dialog appears. You must add at least one member to the group.



Add Member Dialog

Is this member a mail user within your organization?

● Yes

○ No

Full Name contains Sol

1 entries found

Mail

spinner@bridge.net

Selected Item

FIGURE 3-8 Add Member Dialog with Yes Button Pressed.

e. If a desired member is a mail user in your organization, click the Yes radio button. If the desired member is not a user in your organization, click No.

Two versions of the Add Member dialog exist. The version that appears will depend on whether you selected the Yes or No radio button.

f. If you are specifying a member who is a user in the organization, perform the following steps:

i. Search for the member's user entry by specifying a portion of the user's full name.

A full name is any of the possible variations of a user's first name, last name, and middle initial. For example, if you want to specify Bernie Miller as a member, you can specify portion of the following full names that appear in Bernie's user entry:

```
Bernard Miller
Bernie Miller
Bernard A. Miller
Bernie A. Miller
```

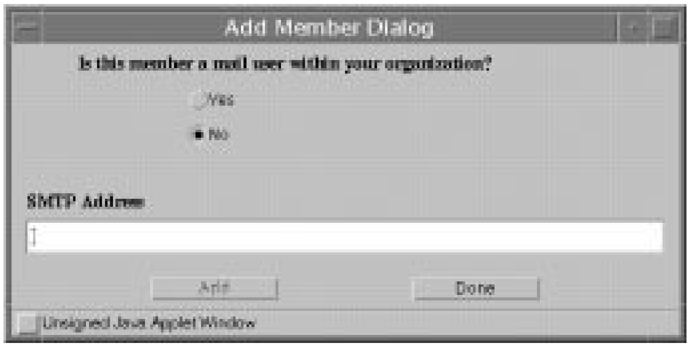
Click the Find button. Once the search is completed, the mail address(es) of the user entry(ies) that match the search parameters appears in the table. Click the address of the desired member. If the search did not yield desired results, perform another search.

ii. **Click the Add button.**

iii. **Repeat the previous two steps for each internal member you want to add.**

iv. **When you are finished adding internal members, click the Done button.**

g. **If you are adding a member who is not a user within your organization, press No button on the Add Member Dialog. the following dialog appears:**



Is this member a mail user within your organization?

○ Yes

● No

SMTP Address

FIGURE 3-9 Add Member Dialog for External Members.

Perform the following steps:

i. **Enter the Internet address of the desired member.**

Enter an address in ASCII characters. You can enter the characters in either uppercase or lowercase. For example: `cstengel@stream.com`

ii. **Click the Add button.**

iii. **Repeat previous two steps for each external member you want to add.**

iv. **When you are finished adding external members, click the Done button.**

h. **To delete a member, click the member entry in the display to highlight it, then click the Delete button.**

9. **Click the Create Group button.**

10. **If finished, click the Done button.**

▼ View a Domain

1. **From the Admin Console home page, click the User Manager icon.**

2. **Select User Manager>Choose Domain to Browse.**

   Enter a fully qualified domain name to view. For example, entering `com` lists all its subdomains. An invalid domain will produce an error message.

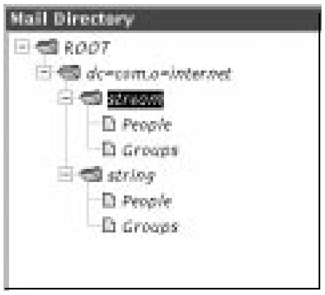


FIGURE 3-10 Viewing Domains

Note – You cannot browse ROOT to view top-level domains such as `.com`, `.org`, `.gov`, or `.edu`. To view a top-level domain (that is, any child of `o=internet`) you must enter the domain name in the Choose Domain to Browse dialog. For example, to view all the `.org` domains, you would enter `org`. Note also that the Mail directory presents a view of the Domain Component (DC) tree, not the OSI tree. If your data is in an OSI tree, SIMS will map it to a DC tree. Refer to the Schema chapter in the *SIMS Reference Manual* for mapping details.

---

3. **Click on the domain folder to view People and Groups.**

▼ To Find and View User/Group Entries

Utility: `imadmin-search-user/group`

AdminConsole>User Manager>User Manager pulldown to Choose Domain to Browse>Highlight People or Groups>Find

1. **From the Admin Console home page, click the User Manager icon.**

2. **Set the Maximum Number of Hits.**

   If there are many thousands of entries in your system, you may wish to limit the number of entries displayed on a search. On the User Manager pull-down, select Configure Maximum Hits and enter the maximum number of entries you would like displayed.

3. **Select the domain and organizational unit (People or Group) that contains entry you wish to view.**

4. **Select User Manager>Choose Domain to Browse.**

   Enter a fully qualified domain name to view. For example, entering `com` lists all its subdomains. Next click the root folder and any subsequent folders to view the domain containing the desired entry to view. Finally click People or Group.

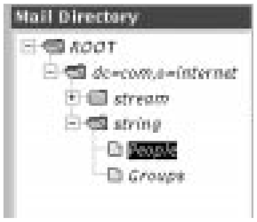


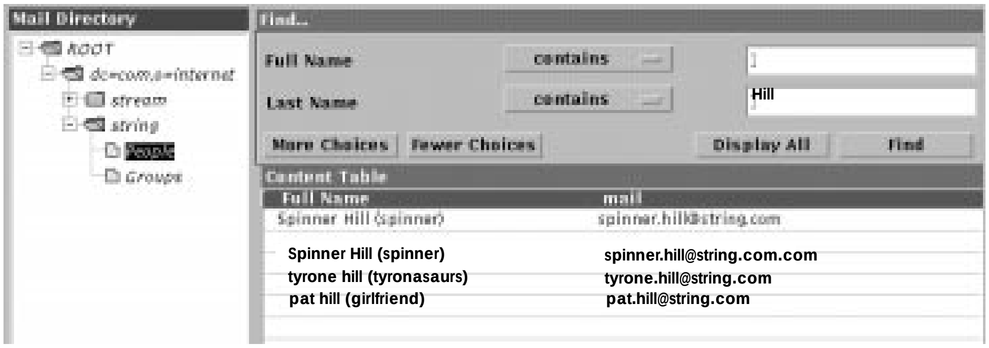
FIGURE 3-11 Browsing the Mail Directory

5. **Type the name or part of the entry you want to view and press Find, or press Display All to display entries without regard to find parameters.**

   Pressing Find or Display All loads the first 50 entries. Load additional entries by scrolling down. The number of entries loaded will equal Maximum Hit. (Maximum Hit can be configured by selecting Configure Maximum Hits from the User Manager pull-down menu. The default is 2000.)

Note – If your browser does not scroll down, and you know you have more than 50 entries, you need to set the security property to low for the browser. See “Preventing the “Warning Applet” Banner” on page 270.

Here we want to view a user entry in `dn:ou=people,dc=string,dc=com,o=internet` with the string `hill`. If you wanted to view a group entry, you would click Group instead of People. You can also search by other parameters. Press More Choices to view these parameters:



Full Name contains

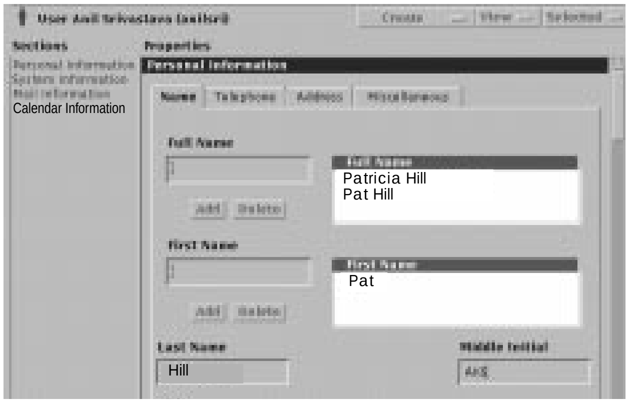
Last Name contains Hill

Full Name	mail
Spinner Hill (spinner)	spinner.hill@string.com
Spinner Hill (spinner)	spinner.hill@string.com.com
tyrone hill (tyronasaurs)	tyrone.hill@string.com
pat hill (girlfriend)	pat.hill@string.com

FIGURE 3-12 Full Find Menu

6. **Once you find the entry you are searching for, double-click the entry.**

   The property book for that particular user or group appears (FIGURE 3-13). This property book is divided into sections that contain information for that particular user or group. For a description of the user entry fields, refer to TABLE 3-3. For modification information, refer to “To Modify a User Entry” on page 41.



Full Name: Patricia Hill, Pat Hill

First Name: Pat

Last Name: Hill

Middle Initial: AnS

FIGURE 3-13 User Property Book

▼ To Delete a User or Group Entry from the Directory

Utility: `imadmin-delete-user/group, imadmin-purge-user/group`

To completely remove a user or group from SIMS you must mark deletion of the user/group's entry from the SIMS directory and run `imadmin-purge-user/group`.

AdminConsole>User Manager>Highlight user>Selected Delete

1. **Display the entry to delete in the Content Table of the User Manager Property Book.**

   See "To Find and View User/Group Entries" on page 38.

2. **Highlight the entry and choose Delete from the selected menu.**

   A dialog box prompts you to confirm the deletion of the entry. Click OK. The entry is now marked for deletion from the SIMS LDAP directory. The entry still exists until the `imadmin-purge-user` command is executed.

3. **Synchronize the cached directory.**

   Even though the entry is removed from the SIMS directory, it still remains in the IMTA directory cache until the cache is synchronized with the SIMS directory. Run an incremental `dirsync` (`imta dirsync`) is to update the IMTA cache after a delete and before a purge. A full `dirsync` (`imta dirsync -F`) is necessary to update the cache following a purge. You can run a full directory synchronization or simply wait until the scheduled `dirsync` occurs.

4. **Remove the user's folders and mailboxes from the mailstore.**

   Wait at least two minutes after running `imta dirsync -F`, then execute the `imadmin-purge-user` or `imadmin-purge-group` utility. This short wait ensures that the message queue is cleared before removing the folders and mailboxes. The `/imadmin-purge-*` command can be run immediately or periodically as desired.

▼ To Modify a User Entry

Utility: `imadmin-modify-user`

A user entry or *user profile* contains information on a user. TABLE 3-3 describes each user entry field. Note that since the entry was already successfully created, no additional fields need to be added for the entry to be operational. This section describes fields that can be modified or added to the entry.

AdminConsole>User Manager>Display then double click the user entry

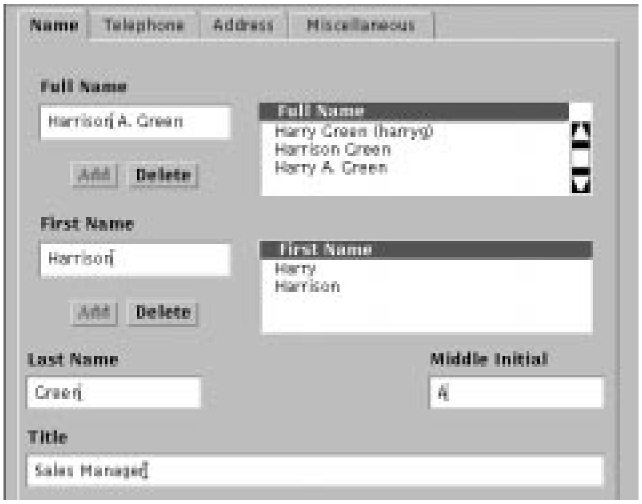
1. **Display the user's Property Book.**

See “To Find and View User/Group Entries” on page 38. The user’s property book contains a number of configurable property fields (see TABLE 3-3 on page 25 for a complete list of fields). The following fields are mandatory:

- Full name
- Last name
- Login name
- Password
- Mail host
- Preferred originator address
- Mail aliases

If you specify the delivery channel type as *Internet* in the Mail Information section, you must also configure Internet mail delivery options. The configuration of all other fields is not required.

2. **Configure the fields in the Name section (**FIGURE 3-14**).**



Full Name: Harrison A. Green

Full Name
Harry Green (harryg)
Harrison Green
Harry A. Green

First Name: Harrison

First Name
Harry
Harrison

Last Name: Green

Middle Initial: A

Title: Sales Manager

FIGURE 3-14 Name Section

The full name and last name fields are required. All other fields in this section are not required.

a. **Enter full name(s).**

You can also enter variations of the full name. Click the Add button under the Full Name field for each full name you enter.

b. **Enter last name.**

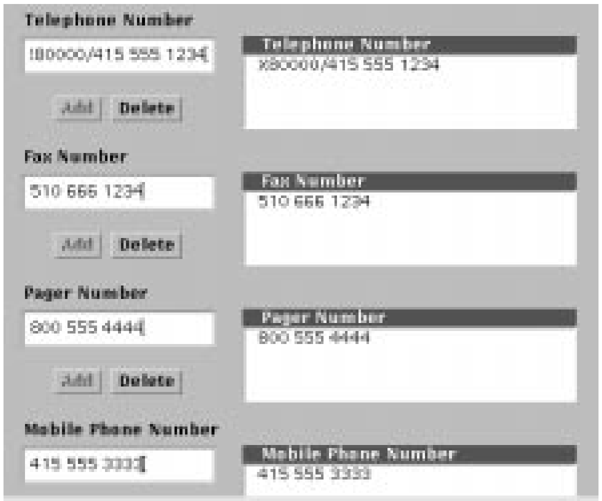
Enter the same last name specified in the full name field.

c. **Optional: Enter the First Name, Middle Initial, and Title Fields if desired.**

For the first name field, you can enter first name variations. For each given name you enter, click the Add button under the First Name field.

3. **Optional: Enter the fields in the Telephone section (see** FIGURE 3-15**).**

Click the Telephone tab. Enter the telephone numbers in any desired syntax. For each entry, click the Add button under the appropriate field.



Telephone Number: 180000/415 555 1234

Telephone Number: X80000/415 555 1234

Fax Number: 510 666 1234

Fax Number: 510 666 1234

Pager Number: 800 555 4444

Pager Number: 800 555 4444

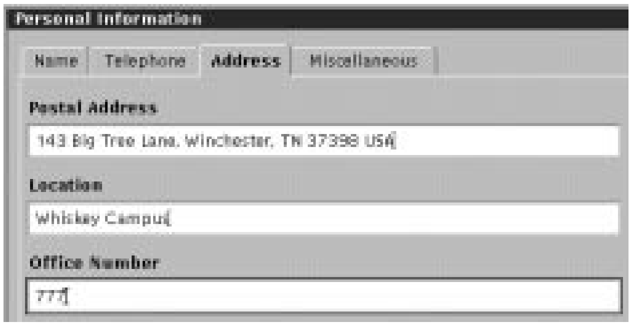
Mobile Phone Number: 415 555 3333

Mobile Phone Number: 415 555 3333

FIGURE 3-15 Telephone Section

4. **Optional: Enter the fields in the Address section.**

Click the Address tab (FIGURE 3-16). Configure the desired fields.



Postal Address: 143 Big Tree Lane, Winchester, TN 37398 USA

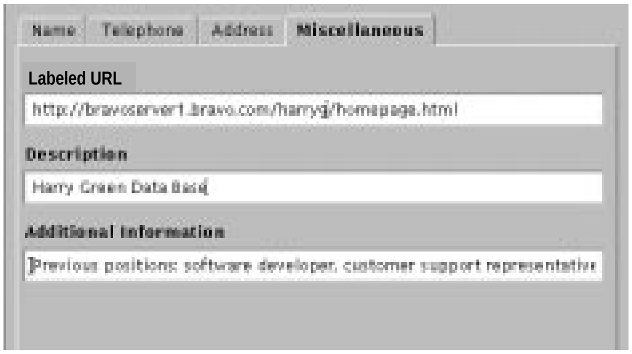
Location: Whiskey Campus

Office Number: 777

FIGURE 3-16 Address Section

5. **Optional: Enter the fields in the Miscellaneous section.**

   Click the Miscellaneous tab (FIGURE 3-17).



Labeled URL
http://bravoserver1.bravo.com/harryg/homepage.html

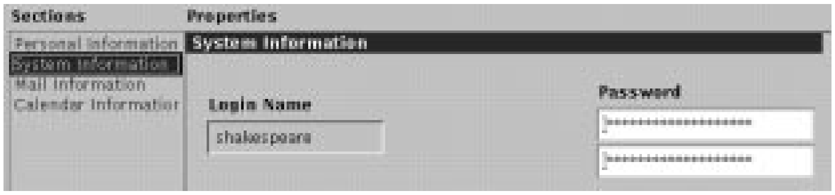
Description
Harry Green Data Base

Additional Information
Previous positions: software developer, customer support representative

FIGURE 3-17 Miscellaneous Section

6. **Configure the fields in the System Information section.**

   Click System Information in the sections list (FIGURE 3-18). The login name and password fields are mandatory.



Login Name
shakespeare

Password
****
****

FIGURE 3-18 System Information Section

a. **Configure the password field.**

   Enter a password for the user in ASCII characters, once in each Password text field. You can enter the characters in either uppercase or lowercase. For example, a valid entry is as follows:

   ```
   Abra_CaDabra
   ```

   For security reasons, the mail server by default stores the password in an *encrypted* or scrambled state. Later, the user can change the default password. (See the *SIMS Delegated Management Guide* for information on how the user can change the mail password.)

   If the group has an existing encrypted password, you can use either of the following syntaxes to load the encrypted password into the mail server:

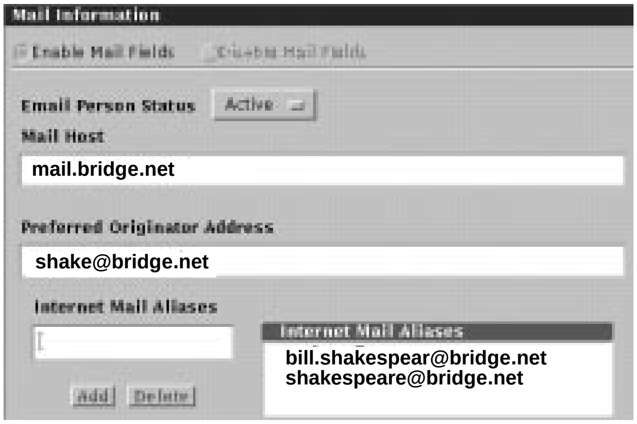
   {crypt}<*password*> or
   {sunds}<*password*> (If you are using the Sun Directory Server)

Refer to the Netscape documentation for the encryptions methods that it supports.

7. **Configure the fields in the Mail Information section.**

Click Mail Information in the Sections list (FIGURE 3-19)

.



Mail Information

● Enable Mail Fields ○ Disable Mail Fields

Email Person Status: Active

Mail Host: mail.bridge.net

Preferred Originator Address: shake@bridge.net

Internet Mail Aliases:

- bill.shakespear@bridge.net
- shakespeare@bridge.net

FIGURE 3-19 Mail Information Section

The mail host and preferred originator address in this section are required. All other fields in this section is not required.

Note – There are two radio buttons labeled Disable Mail Fields and Enable Mail Fields in the mail information section. If an entry is defined as a calendar-only user, then the Mail Information section will be disabled. Later, if you wish to change the entry to support mail, you can click the Enable Mail Fields button and enter mail information in this section.

---

a. **Set user status.**

Status can be set to Active (user’s account is active and the user may use all service granted) or Inactive (user’s account is inactive and the user may not use any services granted; service requests for a user marked as Inactive return transient failures). Inactive maybe used to suspend usage of the group without actually deleting the group entry or mailbox.

b. **Configure the mail host field.**

Enter the host name, including the full domain name, of the user’s mail server in ASCII characters. Enter the characters in lowercase. For example, if the host name for user Harry Green’s mail server is `mailserver1` and this mail server exists in the `stream.com` domain, then the following is a valid entry:

```
mailserver1.stream.com
```

c. **Configure the preferred originator address field.**

Enter the email address that a recipient within the email system will see when a message from the user is received. Enter the address in uppercase or lowercase ASCII characters. The format of the address must be in RFC 822 format:

```
harry.green@mailserver1.stream.com
```

d. **Configure the mail aliases field.**

Enter alternate email aliases, if any, defined for the user. Mail to this alias will be delivered to the user associated with this entry. The value in this attribute must be unique in the domain. Example:

```
harryg@stream.com
```

Click the Add button under the mail aliases field for each address that you enter.

8. **If necessary configure the Internet Delivery Options (**FIGURE 3-20**).**

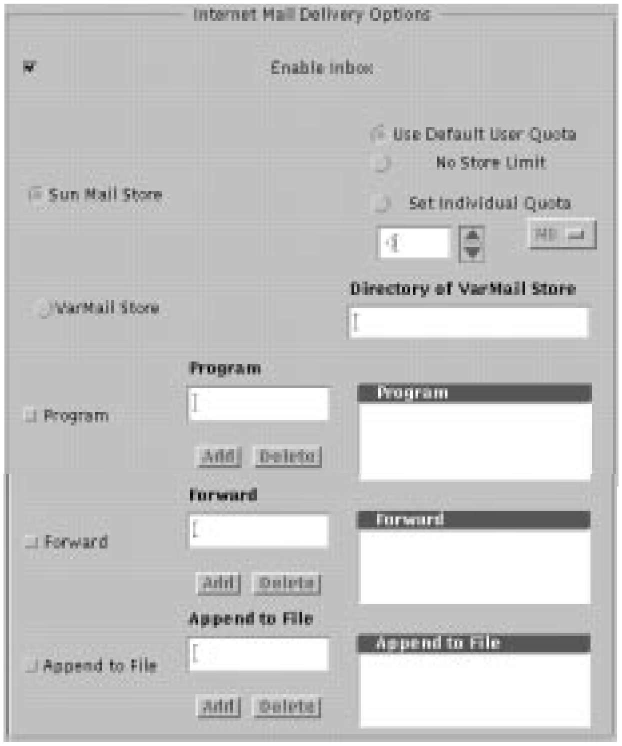


FIGURE 3-20 Internet Mail Delivery Options (Composite Picture)

a. **Check Enable Inbox to enable reading of mail.**

b. **Press which message store the user's Inbox will reside in.**

Click the radio button for either the Sun Message Store or `/var/mail` (VarMail Store). We highly recommend the Sun Message Store as it is more secure, more space efficient, more centralized, and much more easy to back up than `/var/mail`.

i. **If you specified the Sun Message Store, set the maximum amount of hard disk space or *quota* that the user's mailboxes can occupy.**

This message store quota only takes effect if the User Quota Enforcement option in the Message Store Property Book is set to On. (See "User Quota Enforcement" on page 168 and "To Configure Advanced Options" on page 170 for details.). The following size limit options are offered:

Use Default User Quota - Default user quota is set in the Advanced Options section of the Message Store Property Book. It is factory set to 20 Mbytes.

No Store Limit - the user has unlimited message store space.

Set Individual Quota - Select a number and the unit of measure (Kilobytes or Mbytes). This quota will not take effect until an incremental or full directory synchronization occurs (see "Alias Synchronization Schedule" on page 87 or see the `dirsync`, `iminitquota`, and `imquotacheck` man pages for more information).

ii. **If you specified that the user's Inbox will reside in `/var/mail`, then a user directory will automatically be created in `/var/mail/<userID>`.**

If you want it to be under some other directory, you need to create it. Any mail sent to the user before the directory is created will be lost.

c. **Optional: Enable the delivery of email to UNIX programs by clicking the Program check box.**

Enter a pre-configured method name defined by the
`imta program -a -m <method name> -p <program name>`
command (see the `imta-program` man page and "To Make Delivery Programs Available to Users" on page 86, and press Add.

d. **Optional: You can enable the forwarding of email to specified addresses by clicking the Forward check box.**

When specifying a forwarding address, use the following syntax:

<user>@<domain>

For example, to forward a message to Harry Green, enter the following:

```
harry.green@stream.com
```

Enter the forwarding address in ASCII characters and press Add. You can enter the characters in either uppercase or lowercase. You can provide multiple forwarding addresses. For each address, click the Add button under the Forward field. (See the *SIMS Delegated Management Guide* for information on how the user can set the forwarding address.)

e. **Optional: You can enable the appending of email to specified files by clicking the Append to File check box.**

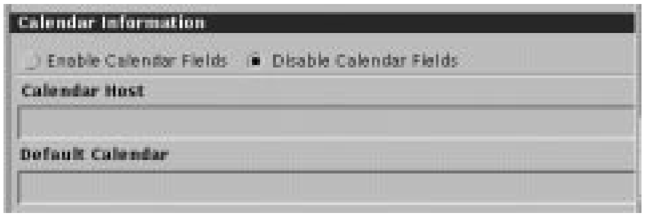
Specify the full path name of the file. For example, you can specify the following:

```
/home/harryg/widget/component.txt
```

The email will be attached to the end of the `component.txt` file. Enter the file name in ASCII characters. You can enter the characters in either uppercase or lowercase. You can provide multiple file names. For each file name, click the Add button under the Append to File field.

9. **Configure the Calendar Information.**

You can add Calendar information to the user entry. This will allow the user to maintain a calendar using the Web Access user application. Click Calendar Information, then click the Enable Calendar radio button and enter the Calendar Host (mandatory) and the Default Calendar (optional). Note that once the Enable Calendar Fields button is pressed, it cannot be "unpressed." The `rpc.cmsd` file must be installed on the calendar host.



Calendar Information

○ Enable Calendar Fields ● Disable Calendar Fields

Calendar Host

Default Calendar

FIGURE 3-21 Calendar Information

If the entry is a *calendar-only* entry, the Internet Mail Delivery Options are disabled. That is, the Disable Mail Field radio button in the Internet Mail Delivery Options section will be pressed. If you press the Enable Mail Field radio button, then you must fill in the mandatory mail configuration fields: mail host, preferred originator address, and mail aliases.

10. **When you have input required and optional fields for a user, click the Apply button at the bottom of the Add User page.**

    If you entered a field incorrectly, an error message will identify the field. Refer to the documentation for the correct syntax and reenter the field. Click either the OK or Apply button.

▼ To Modify a Group Entry

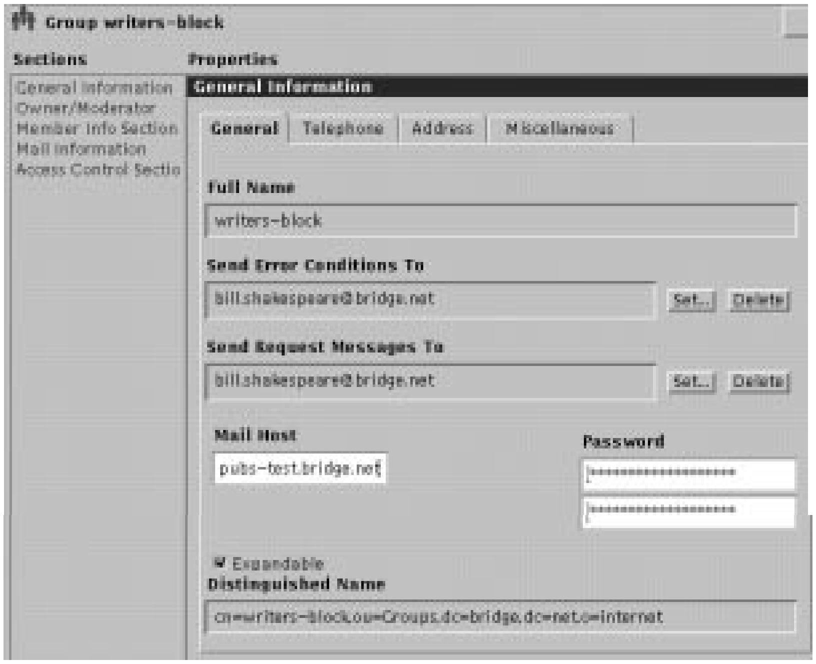
Utility: `imadmin-modify-group`

A group or *distribution list* entry contains information about a distribution list. TABLE 3-3 describes each group entry field and whether a field is required or optional.

AdminConsole>User Manager>Display the Group Entry and double click on it.

1. **Display the group entry property book.**

See “To Find and View User/Group Entries” on page 38. The group’s attributes are displayed as fields. You can modify fields or enter fields not previously entered. For a description of each of the group entry fields, refer to TABLE 3-4.



Full Name
writers-block

Send Error Conditions To
bill.shakespeare@bridge.net

Send Request Messages To
bill.shakespeare@bridge.net

Mail Host
pubs-test.bridge.net

Password
****
****

☑ Expandable

Distinguished Name
cn=writers-block,ou=Groups,dc=bridge,dc=net,o=internet

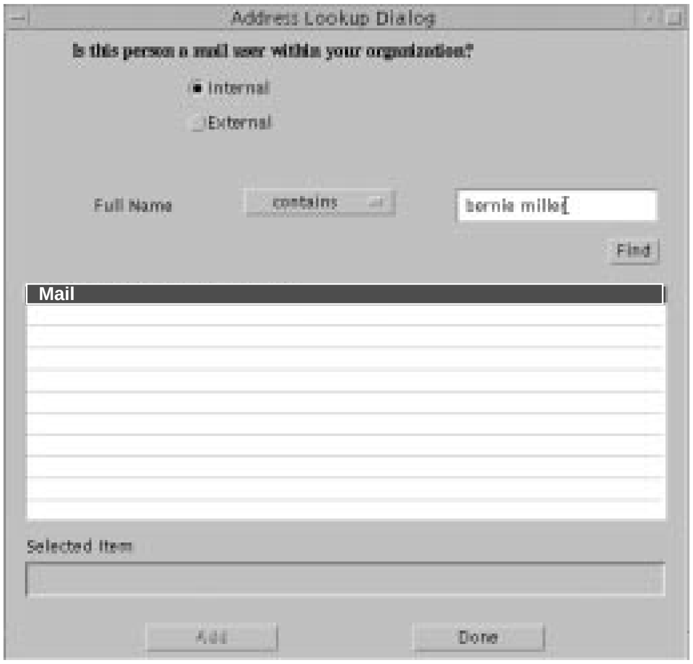
FIGURE 3-22 Group Entry Property Book—General Information.

2. **Modify the fields in the General Information section as desired (**FIGURE 3-22**).**

   a. **Full Name cannot be modified.**

   b. **Enter the Send Error Conditions To and the Send Request Messages To fields.**

   Send Error Conditions To specifies the address to which to send a message if a distribution list error condition arises. The Send Request Messages To field specifies the address to send messages containing requests to be added to the distribution list. Click the Set button next to the desired field. The Address Lookup dialog appears. If the individual to which you want error condition or request notices sent is a mail user within your organization, click the Internal radio button at the top of the dialog (FIGURE 3-23). If the individual is not within your organization, click the External radio button (FIGURE 3-24).



Address Lookup Dialog

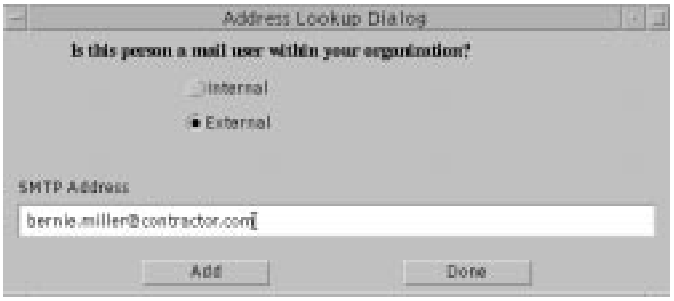
Is this person a mail user within your organization?

● Internal

○ External

Full Name: contains — bernie miller

FIGURE 3-23 Internal Address Lookup Dialog



Address Lookup Dialog

Is this person a mail user within your organization?

○ Internal

● External

SMTP Address: bernie.miller@contractor.com

FIGURE 3-24 External Address Lookup Dialog

To specify someone in your organization, search for their mail user entry by specifying their full name or a portion of it and then clicking the Find button to display a list of matches. If the search did not yield desired results, perform another search. Click the address of the desired user and click Add.

To specify someone outside your organization, enter their Internet address in either uppercase or lowercase ASCII characters. Click the Add button.

Pressing the delete button will remove the entry from the corresponding field. Pressing Apply after making those entries blank will send error and request messages to the originator.

c. **Configure the mail host field.**

The host name should be the fully qualified name of the group's mail server in lowercase ASCII characters.

d. **Configure a password.**

Enter a default password for the group and the shared mailbox, if applicable, in ASCII characters. Enter the characters in either uppercase or lowercase. For example:

```
Abra_CaDabra
```

This password is required when attempting to modify the group entry fields using the `imadmin-modify-group` command. For security reasons, the mail server by default stores the password in an *encrypted* or scrambled state.

Later, the group can change the default password using the email user's configuration interface. (See the *SIMS Delegated Management Guide* for information on how the user can change the mail password.)

If the group has an existing encrypted password, you can use either of the following syntaxes to load the encrypted password into the mail server:

{crypt}<*password*>   or
{sunds}<*password*>   (If you are using the Sun Directory Server)

e. **Make the member list accessible to all users if desired.**

Click the check box labeled Expandable to make the distribution list members accessible to all users. Users can use the SMTP EXPN command to expand (get the membership of) distribution lists. If not checked, SMTP will have an Access to List Denied message.

3. **Optional: Enter the fields in the Telephone section.**

Click the Telephone tab to display the Telephone section (FIGURE 3-25). Enter the desired fields. You can provide multiple entries for each field in this section. For each entry, click the Add button under the appropriate field.

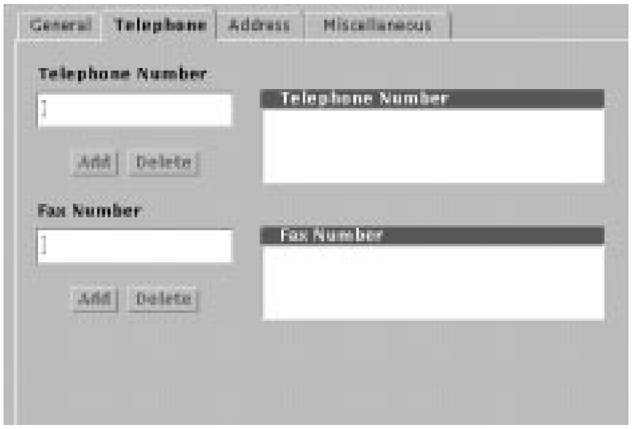


FIGURE 3-25 Telephone Section

4. **Optional: Configure the fields in the Address section.**

   Click the Address tab to display the Address section and fill in the address as desired.

5. **Optional: Complete the fields in the Miscellaneous section if desired.**

   Click the Miscellaneous tab in the General Information (FIGURE 3-26.)

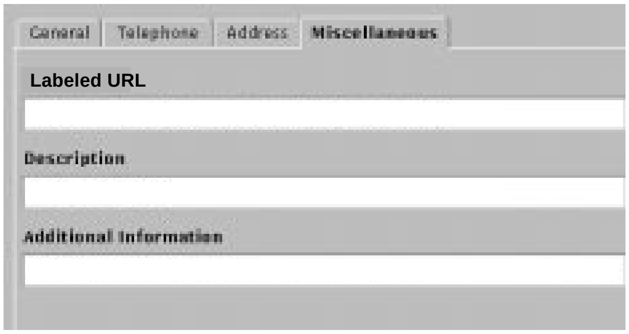
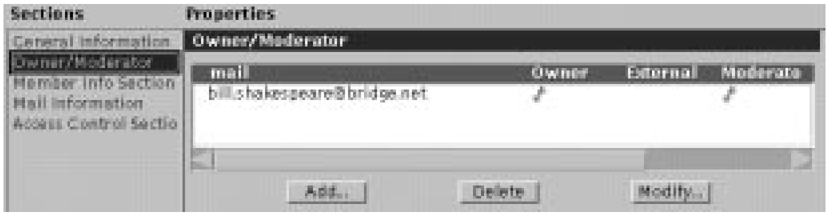


FIGURE 3-26 Miscellaneous Section

6. **Configure the fields in the Owner/Moderator section.**

   Click Owner/Moderator (FIGURE 3-27).



mail	Owner	External	Moderato
bill.shakespeare@bridge.net	✓		✓

FIGURE 3-27 Owner/Moderator Section

An *owner* is an individual who is responsible for a distribution list. An owner can add or delete distribution list members and must be a local email user. A *moderator* is an individual, usually the owner of the distribution list, who initially receives a message addressed to a distribution list. Upon receipt of a message, the moderator can forward the message to the distribution list, edit the message, and then forward it to the distribution list, or not forward the message to the distribution list. A moderator can be local or non-local. *External* indicates that the address is not local to the mail system.

Although a distribution list is created with an owner, you can configure a group as moderator only. Both owner and moderator fields are not required.

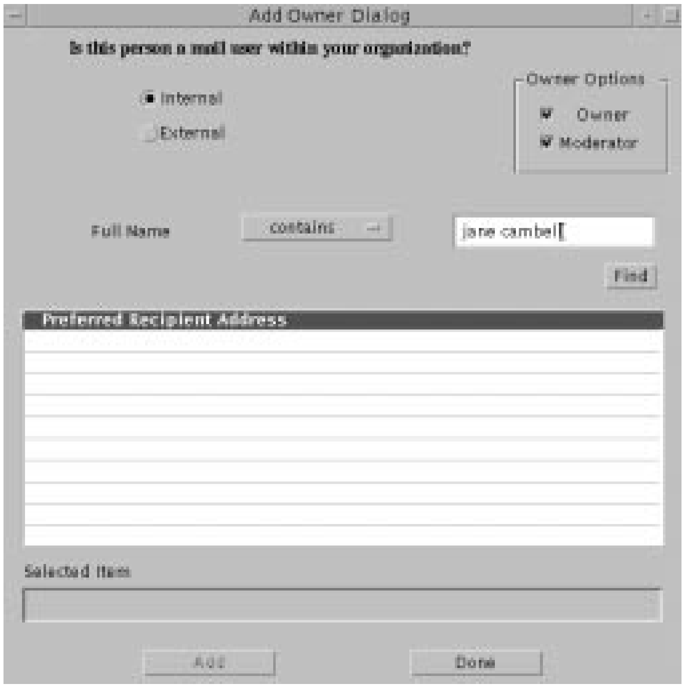
a. **To modify an existing owner/moderator, click the Modify button.**

   Click the check boxes labeled Owner and Moderator to modify the role(s) of the existing owner as appropriate. Click the Add button.

b. **To delete an existing owner/moderator, click the owner/moderator entry in the Owner/Moderator screen to highlight it, then click the Delete button.**

c. **To configure an owner/moderator for the group, click the Add button.**

i. **If the group owner/moderator is a user in the email system, click the radio button labeled Internal.** FIGURE 3-28 **is displayed. If the group owner/ moderator is not configured as a user in the email system, click the External button.** FIGURE 3-29 **is displayed.**



Add Owner Dialog

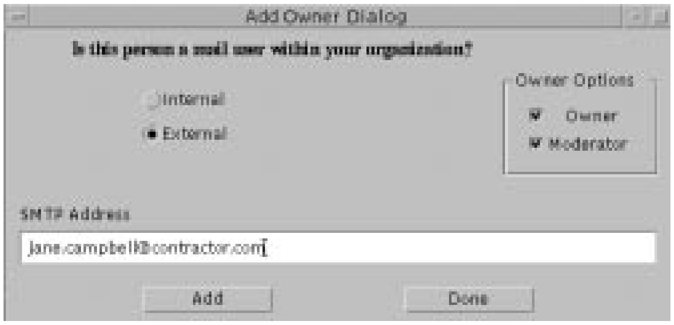
Is this person a mail user within your organization?

● Internal
○ External

Owner Options
☑ Owner
☑ Moderator

Full Name contains jane cambell

FIGURE 3-28 Internal Add Owner Dialog



Add Owner Dialog

Is this person a mail user within your organization?

○ Internal
● External

Owner Options
☑ Owner
☑ Moderator

SMTP Address: jane.campbell@contractor.com

FIGURE 3-29 External Add Owner Dialog

ii. **If the owner/moderator is a local user, perform a search for her entry by entering her name or a portion of it and clicking the Find button. Click the preferred recipient address of the desired owner/moderator. If the search did not yield desired results, perform another search.**

Click the check box labeled owner. If desired, click the check box labeled moderator.

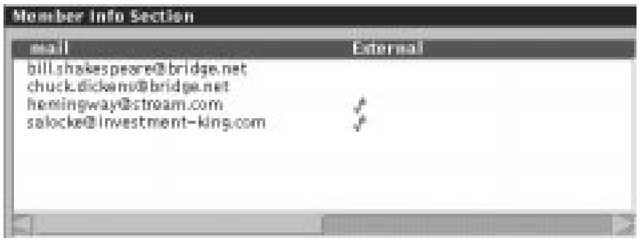
Click the Add button.

iii. **If the owner/moderator is not in the local email system, specify her Internet address.**

Enter the address and click the check box labeled moderator. Note that group owners must be local. Click the Add button. Press Done when finished.

7. **Add or delete members to the group.**

Click Member Info Section (FIGURE 3-30).



mail	External
bill.shakespeare@bridge.net	
chuck.dickens@bridge.net	
hemingway@stream.com	✓
salocke@investment-king.com	✓

FIGURE 3-30 Member Info Section

a. **To delete an existing member, click the member entry in the Member screen to highlight it, then click the Delete button.**

b. **To add group members, click the Add.**

i. **If the desired member is a user in the local email system, click the radio button labeled Internal.**

An internal Add Member Dialog is displayed (see FIGURE 3-23 on page 51). If the desired member is not configured as a user in the email system, click the External button to display external Add member dialog (see FIGURE 3-27 on page 54).

ii. **If the desired member is a local user, perform a search for her entry by entering her name or a portion of it and clicking the Find button.**

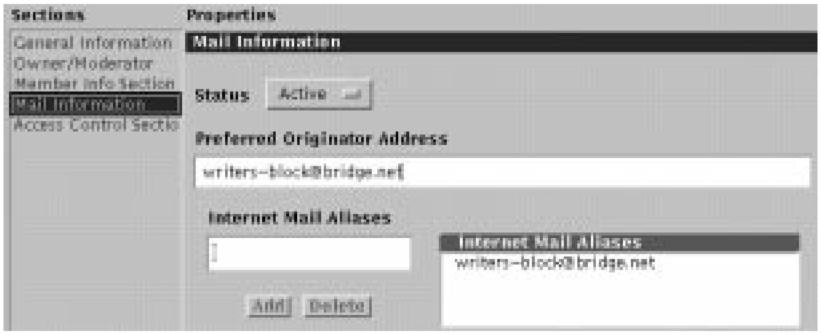
Click the address of the new member. Click the Add button and repeat this step for each member you want to add to a group. If the search did not yield desired results, perform another search.

iii. **If the member is not part of the local email system, enter her Internet address and click Add.**

Repeat this step for each member you want to add to the group.

8. **Optional: Set Group Status, Preferred Originator Address, and Mail Aliases.**

Click Mail Information.



Status Active

Preferred Originator Address

writers-block@bridge.net

Internet Mail Aliases

writers-block@bridge.net

FIGURE 3-31 Mail Information Section

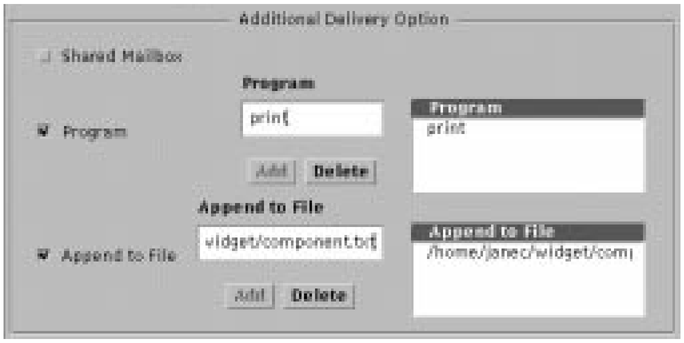
a. **Status** can be set to Active (group's account is active and the group may use all service granted) or Inactive (group's account is inactive and the group may not use any services granted; mail sent to a group is marked as Inactive and returned as a transient failure) using the pulldown menu. Inactive maybe used to suspend usage of the group without actually deleting the group entry or mailbox.

b. **Preferred Originator Address** is the address replicated when a member presses Reply in his mail client software.

c. **Internet Mail Aliases** are alternative email addresses to which mail can be sent to the group. Add or delete as desired.

9. **Optional: Configure the fields in the Additional Delivery Options section.**

Click Additional Delivery Options (FIGURE 3-32) to send mail to a shared mailbox, to a UNIX program, or to append mail to a file.



□ Shared Mailbox

☑ Program

Program: print

Program
print

☑ Append to File

Append to File: widget/component.txt

Append to File
/home/janec/widget/com

FIGURE 3-32 Additional Delivery Options Section

a. **If the messages will be delivered to a shared mailbox in the Sun Message Store, click the check box labeled Shared Mailbox.**

Members can only access the shared mailbox from an IMAP server, and by entering the mailbox name as follows: `#shared/<`*`distribution list name`*`>`. Note that messages are also delivered to each user as will as each group member.

b. **To enable the email delivery to UNIX programs, click the Program checkbox.**

Enter a preconfigured method name defined by the
`imta program -a -m <`*`method name`*`> -p <`*`program name`*`>`
command (See the `imta-program` man page and "To Make Delivery Programs Available to Users" on page 86).

c. **To append email to specified files, click the Append to File check box.**

Specify the full pathname of the file. For example, you can specify the following:

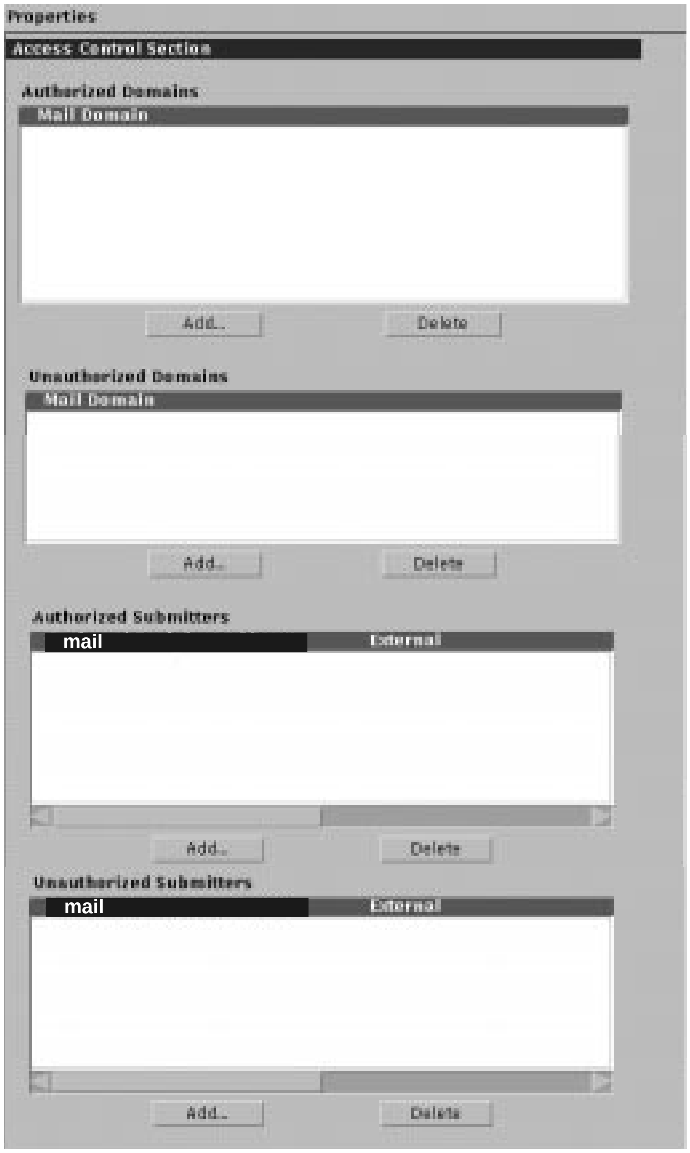
```
/home/janec/widget/component.txt
```

The email will be attached to the end of the `component.txt` file. You can provide multiple file names. For each file name, click the Add button under the Append to File field.

10. **Optional: Configure the fields in the Access Control section.**

    These fields block specified domains and users from sending messages to the group. If nothing is specified, anyone can send messages to the list. If a moderator is created, the message first goes to the moderator. Without a moderator, the message goes to all group members.

    To configure access control, click Access Control to set these attributes.



Properties

Access Control Section

Authorized Domains

Mail Domain

Unauthorized Domains

Mail Domain

Authorized Submitters

mail	External

Unauthorized Submitters

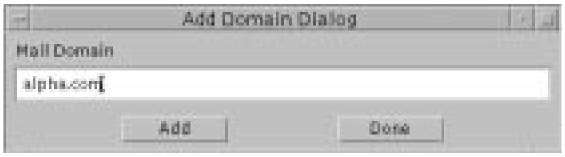
mail	External

FIGURE 3-33 Group Entry Access Control Section

a. **To delete an existing domain or submitter, highlight the entry, click Delete.**

b. **To add an authorized or unauthorized domain, click the Add button below either the Authorized or Unauthorized Domain screen.**

The Add Domain dialog appears as shown in FIGURE 3-34. Enter the unauthorized domain and click Add. Note that you can use the wildcard character (*) as part of the specified domain.



Add Domain Dialog

Mail Domain

alpha.com

FIGURE 3-34 Add Domain Dialog

c. **To add an authorized or unauthorized submitter, perform the following steps:**

i. **If the submitter is a user in the local email system, click the radio button labeled Internal.**

An internal Add Submitter Dialog is displayed (seeFIGURE 3-23 on page 51). If the desired member is not configured as a user in the email system, click the External button to display external Submitter Dialog (see FIGURE 3-24 on page 51).

ii. **If the desired member is a local user, perform a search for her entry by entering her name or a portion of it and clicking the Find button.**

Click the address of the new member. Click the Add button and repeat this step for each submitter to add to the list. If the search did not yield desired results, perform another search.

If you want to specify all members of the distribution list, you can specify the full name of the entry.

iii. **If the owner is not part of the local email system, enter her Internet address and click Add.**

Repeat this step for each member to add to the list. If you are specifying a submitter who is not a configured user or group in the email system, specify the Internet address of the desired submitter.

11. **After you have made your desired changes, click the Apply button at the bottom of the Group dialog.**

If you entered a field incorrectly, an error message will identify the field. Refer to the documentation for the correct syntax and reenter the field. Click Apply button.

CHAPTER **4**

Hosted Domains

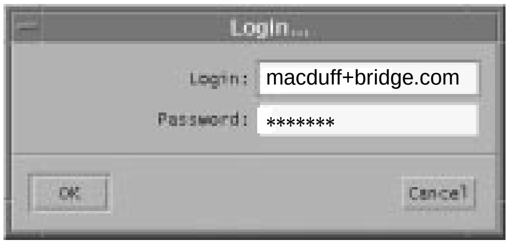
This chapter describes how to create, delete, and modify hosted domains, how to create and remove hosted domain delegated administrators, and how to customize the Delegated Admin Console.

TABLE 4-1 Hosted Domain Topics and Tasks

Topic/Task	Description	Page
Mail Client Login to Hosted Domains	How users log in to a hosted domain	62
Creating, Viewing, Deleting, and Modifying a Hosted Domain	How to create, delete and modify hosted domains.	63
Creating, Viewing and Removing Delegated Administrators and Postmasters	How to create and remove delegated administration privileges.	71
User Administration	Refer to the *SIMS Delegated Management Guide*.	71
Delegated Management Console Customization	Customization of the Delegated Management Console.	73

Mail Client Login to Hosted Domains

To access mailboxes users must enter their user ID, separator (default is +), and their domain, along with their password. In the example below, the user name is `macduff` and the domain is `bridge.com`.



Login: macduff+bridge.com

Password: *******

FIGURE 4-1 Example Login

Note – Users in the default domain do not need to enter their domain name to access their mailboxes. They only need to enter their user ID name. The default domain is the first domain created upon installation. Do not change the default domain after installation as this can cause problems in the message store.

▼ Changing the Default Separator

The default message access login separator is +. It can be changed by modifying the `loginSeparator` in the `$BASEDIR/etc/opt/SUNWmail/sims.cnf`, but it **MUST** be done before SIMS deployment. Once the separator is changed, email that has been stored under the previous separator will no longer be accessible. Refer to the `sims.cnf` man page.

▼ Allowing Users in Subdomains to Log In Using the Domain Name

When a hosted domain is created, the default set up is such that users must enter their fully qualified domain name to access their mailbox. For example, a user called `wallyboy` in the domain `mktg.bridge.com` would log in using `wallyboy+mktg.bridge.com`. A user called `superbryn` in the domain `creative.bridge.com` would use `superbryn+creative.bridge.com`. If you want to set up the system such that users in any subdomain of `bridge.com` can login as `<uid>+bridge.com` change the `simsRecursive` attribute in the `dn:dc=stream,dc=com,o=internet` to 1.

Note that you will have to create three sets of re-write rules to complete message delivery, one for each domain. `bridge.com`, `mktg.bridge.com` and `creative.bridge.com`.

Creating, Viewing, Deleting, and Modifying a Hosted Domain

You can create hosted domains using the SIMS Admin Console, by modifying the LDAP directory (see the *SIMS Provisioning Guide*), or using the `imadmin-create-domain` utility. When SIMS is first installed, it will have a single domain in the DIT. FIGURE 4-2 shows the DIT of our Bridge example immediately after installation.

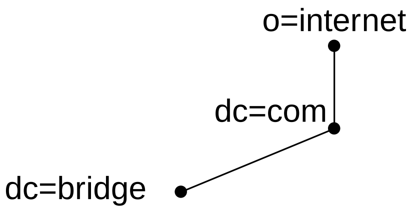


FIGURE 4-2 Bridge DIT After Installation

In the instructions that follow, we will explain how to create two example hosted domains called `stream.com` and `bridge.com`. The DIT will then appear as shown in FIGURE 4-3.

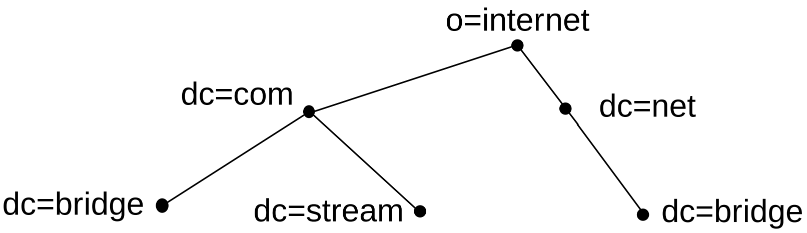


FIGURE 4-3 Bridge DIT After Adding Two Hosted Domains

Note – Hosted mail domains need to correspond with your Domain Name System (DNS). For example, if you add a domain named `eng` to the DIT of the Bridge-ISP Corporation, then the mail domain `eng.bridge.com` needs to exist in Bridge's DNS.

▼ To Create an Hosted Domain

Utility: `imadmin-create-domain`

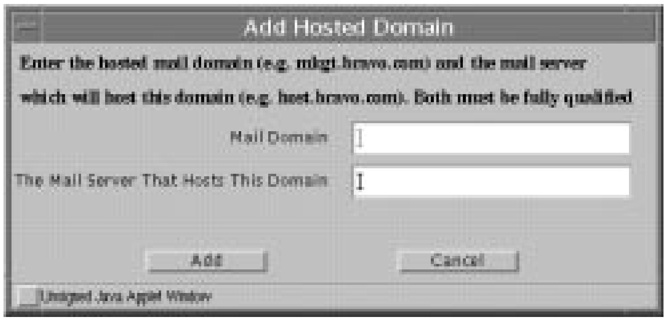
Unlike the `imadmin-create-domain` command, creating a hosted domain with the Admin Console does not also allow you to create a Delegated Administrator. To do this you must use the `imadmin-add-admin` utility. In this example, the default domain (the domain specified at install) is `bridge.com`. We will describe how to create two example hosted domains called `stream.com` and `bridge.com`.

AdminConsole>User Manager>Create pulldown>Domain

1. **From the Admin Console home page, click the User Manager icon.**

2. **Click the Create pull-down menu and select Domain.**

   The following dialog appears:


Add Hosted Domain
Mail Domain
The Mail Server That Hosts This Domain
Add
Cancel
Unsigned Java Applet Window

Enter the hosted mail domain (e.g. mkgt.bravo.com) and the mail server which will host this domain (e.g. host.bravo.com). Both must be fully qualified

FIGURE 4-4 Add Hosted Domain Dialog.

Mail Domain is the fully qualified mail domain that you want to create. Example: `bridge.com`.

Note – If you entered a domain such as `green.org`, SIMS would create the domain `org` automatically. However, you will not be able to delete `org` from the Admin Console. You would have to use and LDAP command. If you created `org` separately, and then created `green` as a child of `org`, you would be able delete both from the Admin Console. Parent domains created in one step (entering `<domain>.<domain parent>` in the Mail Domain Field) cannot be deleted or viewed.

Mail Server is the fully qualified host name of the machine supporting the hosted domains. In this example it might be `mailserver19.bridge.com`.

Note – You can only create hosted domains that are children of the top-level domain components (those under `o=internet` such as `org`, `gov`, and `edu`). When you create a hosted domain, if a parent domain does not exist SIMS will create one.

---

3. **Enter the desired information in the dialog box and click Add.**

   The mail domain is created along with a People and Groups container. A SIMS administrator can now create user entries in this mail domain. To view the domain select **User Manager>Choose Domain to Browse.**

4. **Create a delegated administrator**

   Creating a hosted domain with the Admin Console does not automatically create a delegated administrator. See "Creating Delegated Administrators" on page 71.

▼ To Create Hosted Domain Alias

Utility: `imadmin-add-alias`, `imadmin-delete-alias` and `imadmin-modify-alias`

There may be a situation in which a hosted domain customer wishes to have an alias for its domain. For example, suppose your domain is `international-basketball-league.com`, but you also wish receive mail sent to `ibl.com`. To create hosted domain aliases, use the `imadmin-add-alias` utility. Refer to the man page for complete details.

Note – Your new domain must be registered with InterNIC in order for it to operational.

▼ To Delete a Hosted Domain

Utility: `imadmin-delete-domain` and `imadmin-purge-domain`

You can mark a domain as deleted from the directory information tree (DIT). This operation deletes all folders and entries contained in that domain. For example, if you delete the domain named `mktg.bridge.com` from the DIT of the Bridge-ISP Corporation, then all user entries in the People folder and all group entries in the Group folder contained in the Marketing domain will be marked as deleted.

AdminConsole>User Manager>Selected domain to delete>Selected-Delete

1. **From the Admin Console home page, click the User Manager icon in the Tasks portion of the page.**

   The User Manager page displays.

2. **In the directory tree highlight the domain label (for example, Marketing), then click the Selected menu and choose Delete.**

   A dialog prompts you to confirm deletion of the domain.

3. **Click OK.**

   Note that this only marks the domain for deletion. The domain cannot be seen on the Admin Console, but it still exists in the DIT until it is purged.

4. **Run** `imadmin-purge-domain`

   See the `imadmin-purge-domain` man page for details.

Modifying a Hosted Domain

Use the `imadmin-modify-domain` utility to modify attributes of a domain's domain entry in the DIT. See the man page and Schema in the *SIMS Reference Manual* for details.

To Set Up the System So that Users Can Log in Without Entering their Domain Name

It is possible to set up virtual hosted domains such that users do not have to include the separator and domain name upon login. This is a complex process involving the configuration of the DNS and server hardware to support multiple IP addresses on a single SIMS server, and configuring the `ims.cnf` file to support IP address-based domain recognition. This technology is referred to as *Domain from IP*.

1. **Setup up your SIMS server to have multiple IP addresses, and give each address a DNS hostname.**

   In this example we add two IP addresses, A_1 and A_2, to the SIMS server (defined in `sims.cnf` as `logicalHostname=mail.bridge.net`). Each each address is givine the hostnames `mail.beam.com` and `mail.stream.com`.

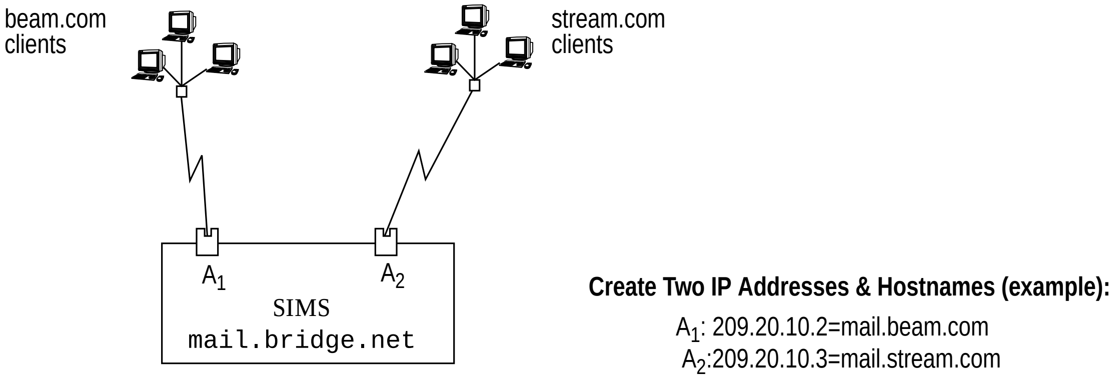
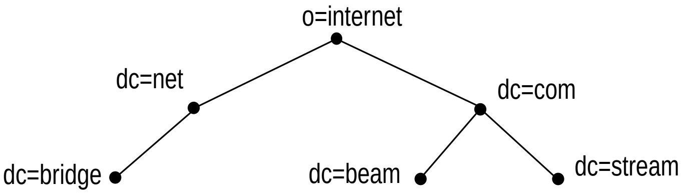

beam.com clients
stream.com clients
A_1
A_2
SIMS
mail.bridge.net
Create Two IP Addresses & Hostnames (example):
A_1: 209.20.10.2=mail.beam.com
A_2:209.20.10.3=mail.stream.com

FIGURE 4-5 Simplified Domain from IP

2. **Create your virtual hosted domain in the directory. (See "To Create an Hosted Domain" on page 64).**

   In this example, our hosted domain is `stream.com`. We use the DNS hostname `mail.stream.com` as the mail host for this domain. The figure below shows the DIT for this example.



3. **List all of the virtual IP addresses in the DNS zone file for the host domain pointing to the logical hostname in `/etc/opt/SUNWmail/sims.cnf`.**

   For example, if your `sims.cnf` file has:

```
logicalHostname=mail.bridge.net
```

   Your DNS zone file needs:

```
mail.bridge.net    IN    A    209.20.10.2
mail.bridge.net    IN    A    209.20.10.3
```

4. **Bind the DNS hostname or IP address to the hosted domain in the `/etc/opt/SUNWmail/ims/ims.cnf` configuration file using the `ims-bind-address` attribute.**

   The format for setting the `ims-bind-address` attribute is as follows:

```
ims-bind-address:[<hostname>[=domain]]
[(<service>=<port1>[,<port2>..]
[:<service>=<port3>[,<port4>..]..])]
```

   `<hostname>` is a hostname or an IP address to listen to when binding sockets in the message-access server. If hostname is not present or the value is equal to '*', listen to all the addresses available.

   `<domain>` is the default search domain associated to this address(es) / port(s). This value supersedes `defaultDomain` from `sims.cnf`.

   `<service>` is one of imap, pop3, imaps, pop3s (if no service is listed, the ports indicated in `/etc/services` are used)

   `<port>[,<port>..]` is one or more TCP port numbers to listen to for the service specified. Specifying 0 means the service not provided on this address)

   The code line for our example would look as follows:

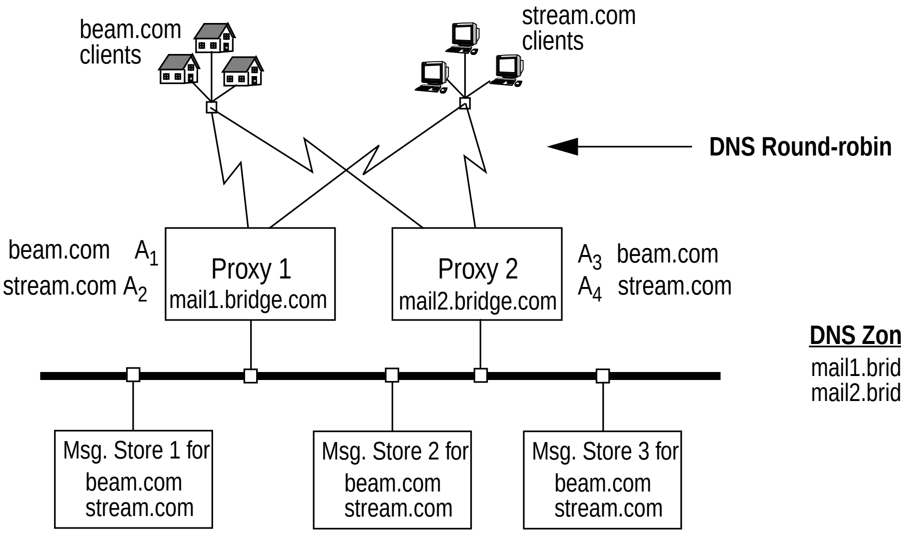
```
ims-bind-address: mail.beam.com=beam.com
ims-bind-address: mail.stream.com=stream.com
```

5. **Restart imaccessd each time you modify `ims.cnf`.**

   Use `/etc/init.d/im.server stop` and use `/etc/init.d/im.server start`.

6. **Make sure all clients point to the new POP server hostname.**

   A more realistic configuration would have multiple proxies and multiple backend messages stores installed as follows. As more hosted domains are added, the DNS configuration gets more complex.



Domains:

beam.com
stream.com

IP Addresses:

A_1:	209.20.10.2
A_2:	209.20.10.3
A_3:	209.20.10.4
A_4:	209.20.10.5

DNS Zone File:

```
mail1.bridge.com  IN  A 209.20.10.2
mail2.bridge.com  IN  A 209.20.10.3
```

DNS Round-robin for beam.com

IP Addr.	Client POP Reference	Server Host Reference*
A_1	mail.beam.com	proxy1-address1.bridge.net
A_3	mail.beam.com	proxy2-address1.bridge.net

DNS Round-robin for stream.com

IP Addr.	Client POP Reference	Server Host Reference*
A_2	mail.stream.com	proxy1-address2.bridge.net
A_4	mail.stream.com	proxy2-address2.bridge.net

*** For reverse DNS Lookups.**

Set up in DNS Environment

ims.cnf Entries for Proxy 1:

```
ims-bind-address:  proxy1-address1.bridge.net=beam.com
ims-bind-address:  proxy1-address2.bridge.net=stream.com
```

ims.cnf Entries for Proxy 2:

```
ims-bind-address:   proxy2-address1.bridge.net=beam.com
ims-bind-address:   proxy2-address2.bridge.net=stream.com
```

FIGURE 4-6 More Complex Domain from IP Configuration

Note – If beam.com contains subdomains and the domain entries has the `simsRecursive` attribute set to 1, then users in subdomains of `beam.com` can also login using their uid (note that the appropriate rewrite rules must also be defined). If `simsRecursive` attribute is set to 0, then they must enter their `uid+subdomain` to access their mailboxes.

Creating, Viewing and Removing Delegated Administrators and Postmasters

A delegated administrator adds, deletes, searches, and modifies user and group entries for a particular domain. Typically a delegated administrator works for the company, owning the domain, at the company's site (as opposed to working at the ISP providing the virtual hosted domain). The delegated administrator performs the administrative tasks using the Delegated Management Console. Refer to the *Delegated Management Guide* for further information.

A domain postmaster is simply a mailbox that receives failed delivery notifications and external requests for addresses. By designating a postmaster to a hosted domain, the SIMS administrator does not have to receive and deal with failed delivery messages and external requests for email addresses. These messages can go to a postmaster mailbox designated at each hosted domain company.

▼ Creating Delegated Administrators

To create a delegated administrator, a SIMS administrator must grant delegated administration privileges to an existing user. Therefore, you must first create a user (see "To Create a User Entry" on page 28) and you must then run the `imadmin-add-admin` utility.

▼ Viewing Delegated Administrators

A list of users who have delegated administrator privileges for a particular domain can be generated with the utility `imadmin-search-admin`

▼ Removing Delegated Administrator Privileges

Delegated administrator privileges can be removed by a SIMS administrator using the utility `imadmin-remove-admin`.

▼ Creating Domain Postmaster Mailboxes

To create a domain postmaster mailboxes, select the mailbox you wish to make a postmaster, then use the add the `imadmin-modify-domain` utility to add the `rfc822postmaster:<uid@domain>` attribute to the domain:

```
# imadmin modify domain -D <SIMS Admin login> -w <password> -A
rfc822postmaster:<uidOfPostmaster@domain> -n <domain>
```

User Administration

User's can perform the following email administrative functions by accessing the User's Delegated Management Console.

- Change password
- Start and stop vacation notice
- Forwarding mail
- Listing distribution lists membership

To access the console, enter http://<SIMS server>/sims/en/emailuser.html in the browser installed with SIMS. Refer to the *SIMS Delegated Management Guide* for more information.

Delegated Management Console Customization

Every company creates customized branding with certain color themes, typefaces, and corporate or product logos. The look of the Delegated Management Console can be customized to better reflect the corporate identity. The graphical elements in the Delegated Management Console can be replaced or redesigned. New elements that did not ship with the product can also be added.

This section points out the graphical elements that may be customized. It also provides customization tips to consider when redesigning or changing these elements.

Structural Tables to Organize the User Interface

HTML tables are used to organize the graphical elements and contents in the Delegated Management Console pages. It is necessary to discuss the underlying table structure because the organization of these tables dictates how the graphical elements align on the page. An illustration of the structural table is shown in FIGURE 4-7. The tables are referred to in the code by the same names given in the illustration.

The HTML code is structured such that an Overall Layout table contains two other main tables used to organize the contents and consistently designate certain areas of the screen for certain functionality. These two tables are the NavBar table, on the left, and the Contents table, on the right. The NavBar table designates the left pane of the screen as the navigation area by organizing navigation buttons vertically in the left pane of the screen. The Contents table designates the right pane of the screen as the content area, where all of the information a user will manipulate appears.

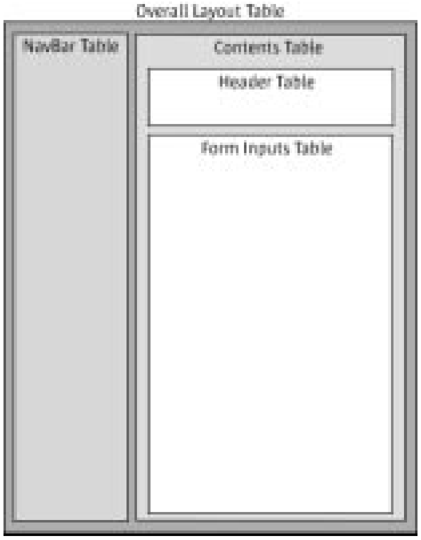


FIGURE 4-7 Structural table of the Delegated Management Console

Background Image

The concept of two panes with distinct functionalities is visually reinforced with a two-color background image (`bkgd.gif`). This background image, which creates the background colors for the page, is placed in the Overall Layout table. The image tiles vertically down the page, producing colored columns that create two visually distinct panes on the screen. The navigation pane, on the left, is dark purple (or the NavBar color). The contents pane, on the right, is a lighter purple (or the Contents color). This visual aid helps reinforce the idea of distinct functionality for different parts of the screen. Every page uses the background image.

NavBar Color
Contents Color

FIGURE 4-8 Background image

Customization Tips

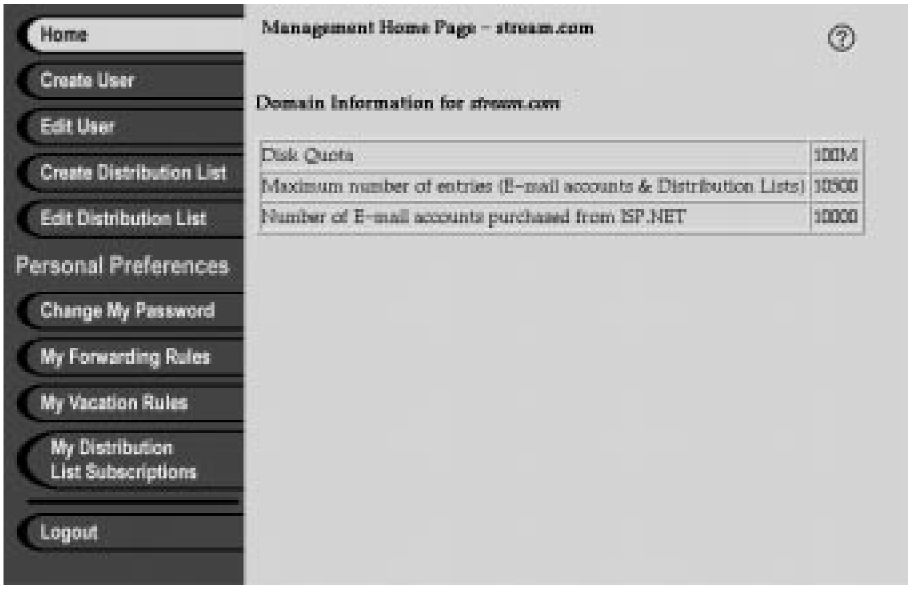
The colors of the background image may be changed to reflect the corporate identity, however the new colors that are chosen should be reused in the navigation buttons.

The content color in the background image will create the content area, so a color should be chosen that ensures good legibility of the text in the content area. For this reason it is recommended to use a darker color for the navigation area and a lighter color for the content area.

The background image, `bkgd.gif`, can be found in the `/opt/SUNWmail/html/`*language*`/graphics` directory.

Navigation Buttons

The interface is designed so that navigation occurs in the left pane of the screen with navigation buttons. These navigation buttons are located in the NavBar Table so that they appear vertically in the left pane of the screen. Each navigation button links to a particular page in the Delegated Management Console.



Management Home Page - stream.com

Domain Information for *stream.com*

Disk Quota	100M
Maximum number of entries (E-mail accounts & Distribution Lists)	10500
Number of E-mail accounts purchased from ISP.NET	10000

FIGURE 4-9 Selected Navigation Button in the Delegated Management Console

The colors, shape, or design of the buttons may be changed to better reflect the corporate identity. It is helpful to understand how the buttons function before editing or manipulating them. The buttons act as tabs. Each button consists of two images: one for an unselected state of the button (`button.gif)` and one for the selected state of the button (`button_select.gif`). An unselected button image is the same color as the NavBar color portion of the background image. When a user selects a button, it changes appearance and becomes the color of the Content color portion of the background image. The selected button now physically connects to the content area, like a tab, and clearly indicates the user's location within the application. The button remains selected as long as the user remains on that page, providing a visual indication of the user's location within the application.

Customization Tips

If the colors of the selected and unselected buttons are changed, the new colors should be used in the background image (`bkgd.gif`) as well in order to retain a working tab model.

If the length of the navigation buttons is changed, the length of the NavBar color in the background image should also be edited. To maintain the tab effect where a selected button changes colors and visually connects with the content area, the right edge of the navigation buttons must align with the right edge of the NavBar color in the background image. The background image is located in the Overall Layout table. Because the navigation buttons are embedded in the NavBar table, which is inside the Overall Table, the buttons are indented, even when table borders and buffering are turned off. This indentation is uncontrollable. Therefore, the NavBar color portion of the background image must be made longer or shorter to accommodate the indentation if the length of the navigation buttons is changed. Keep in mind also that different browsers indent tables differently and that the design should be tested in multiple browsers on multiple platforms.

If the text labels on the buttons are changed, maintain consistent naming between the selected and unselected states of each button. The label on the buttons should correspond to the page titles within the Delegated Management Console.

A light font color should be chosen for the labels on the unselected buttons. The font color should provide ample contrast to the button color for good legibility. The Delegated Management Console uses white text on dark purple buttons.

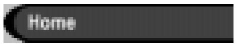


FIGURE 4-10 Unselected button with light color font

A dark color should be chosen for the labels on the selected buttons. The font color should provide ample contrast to the button color for good legibility. The Delegated Management Console uses black text on lighter purple buttons.

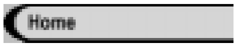


FIGURE 4-11 Selected button with dark color font

The navigation buttons (`button.gif` and `button_select.gif`) can be found in the `/opt/SUNWmail/html/<locale>/graphics` directory.

Product Name and Logos

A banner image with the product name and Sun logo (`banner.gif`) is located in the Overall Layout table. This banner appears on every screen in the Delegated Management Console and can be replaced. The current banner is 600x36 pixels, but the size (as well as the colors and the text) may be altered.

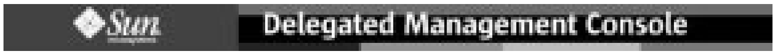


FIGURE 4-12 Banner with Sun logo and product name

Customization Tip

The dimensions and locations of the Sun logos can be used as guidelines for inserting a new logo. The Sun logo in the banner is 166x36 pixels in size.

The banner image (`banner.gif`) can be found in the `/opt/SUNWmail/html/<locale>/graphics` directory.

Graphics Available For Customization

All of the graphics available for customization in the Delegated Management Console are listed in TABLE 4-2. The table lists the name of the graphic along with the name of the GIF file. The `/opt/SUNWmail/html/<locale>/graphics` directory is created when SIMS is installed. This is the directory where all the graphics files are placed. When the CGI program runs, it picks up the graphics from this directory. Therefore, any customized graphics must be saved here as well.

To customize a graphic:

1. Use the graphic from the `/opt/SUNWmail/html/<locale>/graphics` directory.

2. Edit the graphic with a graphics editor, or create a new graphic.

3. Save the graphic back into the `/opt/SUNWmail/html/<locale>/graphics` directory.

For example, if you wish to customize the banner graphic, start with the existing banner graphic, `banner.gif`, from the `/opt/SUNWmail/html/<locale>/graphics` directory. Make modifications with a graphics editor, and save the modified banner graphic back into the

/opt/SUNWmail/html/<locale>/graphics directory. If you do not want to overwrite the original graphic shipped with the Delegated Management Console, save the modified graphic with a new name.

TABLE 4-2 Delegated Management Console Graphics

Image Name	GIF File Name
Banner	banner.gif
Background image	bkgd.gif
Page Help icon (24x24 pixels)	help24.gif
Field Help icon (16x16 pixels)	help16.gif
Properties icon	properties17x17.trans.gif
Optional icon	optional.gif
Search icon	search.gif
Subscribe to Distribution List icon	subscribe17x17.trans.gif
Unsubscribe from Distribution List icon	unsubscribe17x17.trans.gif
View Members icon	view_members17x17.trans.gif
Delete icon	delete.gif
Navigation Bar Graphics	
Home button (unselected)	home.gif
Home button (selected)	home_select.gif
Create User button (unselected)	createuser.gif
Create User button (selected)	createuser_select.gif
Edit User button (unselected)	edituser.gif
Edit User button (selected)	edituser_select.gif
Create Distribution List button (unselected)	createdl.gif
Create Distribution List button (selected)	createdl_select.gif
Edit Distribution List button (unselected)	editdl.gif
Edit Distribution List button (selected)	editdl_select.gif
Personal Preferences Divider	prefhead.gif
Change password button (unselected)	chpswd.gif
Change password button (selected)	chpswd_select.gif
Forward Rules button (unselected)	fwdrules.gif
Forward Rules button (selected)	fwdrules_select.gif

TABLE 4-2 Delegated Management Console Graphics *(Continued)*

Image Name	GIF File Name
Vacation rules button (unselected)	`vacrules.gif`
Vacation rules button (selected)	`vacrules_select.gif`
Subscribe to Distribution List button (unselected)	`dlsub.gif`
Subscribe to Distribution List button (selected)	`dlsub_select.gif`
Separator line	`separator.gif`
Logout button	`logout.gif`

General Design Tips

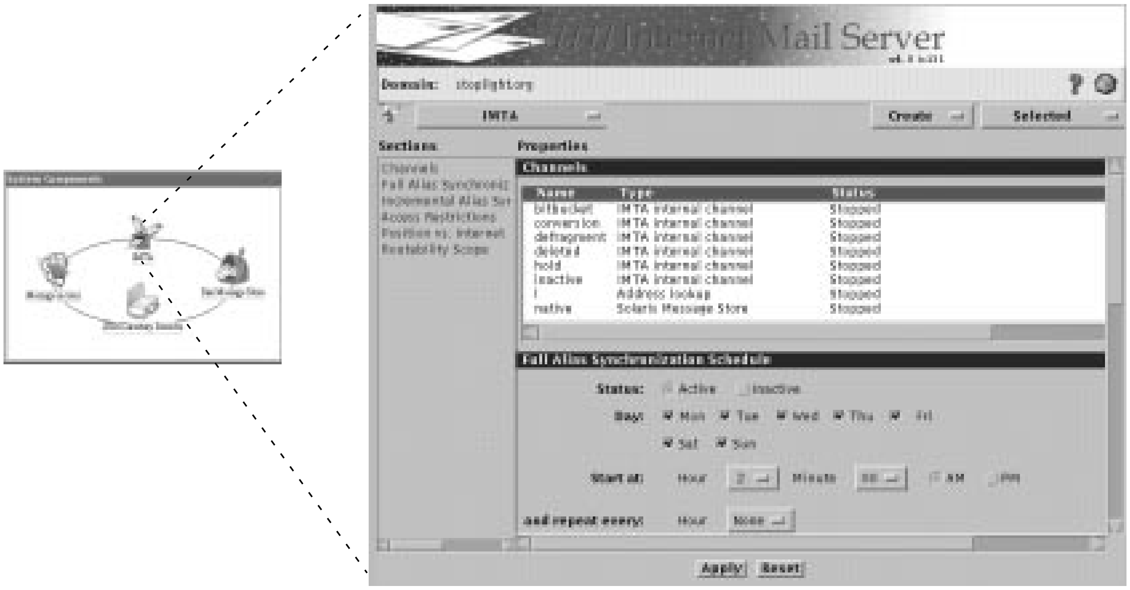
When altering or creating new graphics to appear in the Delegated Management Console, be sure to create the graphics using the so-called “web-safe” color palette. While there is some disagreement about whether the web-safe palette is actually safe, using it may ensure that graphics appear more consistently across various platforms.

To allow for future flexibility to change the background colors and color themes of the Delegated Management Console, design all images as transparent gifs. Avoid transparent gifs with “halos” around them by not dithering the gif to a background color.

CHAPTER **5**

Internet Message Transport Agent (IMTA) Administration

This chapter provides step-by-step instructions for changing the message transport characteristics of the Sun Internet Mail Server (SIMS). To start, bring up the IMTA property book pages.



Channels

Name	Type	Status
bitbucket	IMTA internal channel	Stopped
conversion	IMTA internal channel	Stopped
defragment	IMTA internal channel	Stopped
deleted	IMTA internal channel	Stopped
hold	IMTA internal channel	Stopped
inactive	IMTA internal channel	Stopped
l	Address lookup	Stopped
native	Solaris Message Store	Stopped

Full Alias Synchronization Schedule

Status: ● Active ○ Inactive

Days: ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat ☑ Sun

Start at: Hour 2 Minute 00 ● AM ○ PM

and repeat every: Hour None

FIGURE 5-1 Internet Mail Transport Agent (IMTA) Property Book

Each *section* displays configurable attributes of a particular IMTA property. The *IMTA* pull-down menu allows you to start or stop the IMTA as well as save or restore IMTA configuration. The *Create* pulldown menu allows you to create new channels. The *Selected* pull-down menu allows you to view a channel's properties; start, stop and delete channels; and monitor the message queue.

IMTA Topics and Tasks

TABLE 5-1 Message Transport Topics and Tasks

Topic/Task	Description	Page
IMTA Maintenance Tasks	Stop, start, and restart the IMTA. Also backup and restore of IMTA configuration.	83
Monitoring Channel Status	View the operating status of the SIMS channels	85
Alternative Delivery Programs	Provide user access to alternative delivery programs.	86
Alias Synchronization Schedule	Schedule when the IMTA directory cache is incrementally or fully updated with the latest directory information in the directory service.	87
SMTP Access and Relay Restrictions	Restrict/limit access or delivery of messages from specified email and IP addresses. Unsolicited bulk email control, limiting email access, and so forth.	123
IMTA Location Relative to Public Internet	Specify location of the IMTA relative to the internet, that is, does outbound mail for external addresses have to be forwarded to a smart host?	90
Routability Scope	Specify to whom IMTA can route messages—users, domains etc.	92
Channels	**This section and its subsections below describe channel configuration.**	**93**
Configuring Channels	Create channels, channel descriptions; configure SMTP router hosts, set character set labels.	94
Message Limitation	Set message size limitations.	101
Delivery Status Notification	Specify how delivery failure message is handled. Configure language of message.	102
Diagnostics Output	Write master/slave diagnostic output to a log file.	105
To Set Recipient Limitation	Specify the maximum number of recipients for a single message at which message processing is deferred on the SMTP channel.	106
Message Logging	Configure channel so that it logs as each message enters and is removed from the queue.	107
Reassembling MIME Messages	Enable the Sun Message Store channel, `/var/mail` channel, and pipe channel to reassemble MIME fragmented messages.	108
Rewrite Rules	Add, delete, or modify channel rewrite rules.	109
Monitoring Channel Queues	Monitor accumulated message traffic statistics for each IMTA channel queue.	112

TABLE 5-1 Message Transport Topics and Tasks *(Continued)*

Topic/Task	Description	Page
Viewing Enqueued Messages	View a list of the messages currently stored in the channel queue.	116
DNS-based Canonicalization	Using DNS to canonicalize addresses	118
IMTA Error Messages	Appendix D, “Error Messages	331

IMTA Maintenance Tasks

Stopping, Starting, and Restarting a Channel or the IMTA

You may need to stop and start, or restart a channel if you reconfigure an attribute of a channel, so that the reconfiguration takes effect. (Typically, when you reconfigure a channel attribute using the Admin Console, you are prompted to restart the channel.)

The interruption of service incurred when issuing an `imta restart` is minimal and rarely experienced by user. However, to minimize the probability of affecting users, it is preferable to plan an `imta restart` during light traffic periods. In general, IMTA channels cannot be restarted, stopped, and started independently. However, IMTA components can be restarted in a selective way.

If the configuration change affects only dequeue operations, use the command `imta restart job_controller` so that the enqueue operations are not affected. If the configuration change affects SMTP channel configuration only, the command `imta restart smtp` should be run. If the configuration change only affects the dispatcher, the command `imta restart dispatcher` should be run.

▼ To Stop And Start the IMTA

Command: `imta-start & imta-stop`

AdminConsole>IMTA>IMTA pulldown>Start IMTA

1. **In the IMTA property book, choose Stop IMTA from the IMTA menu.**

   The IMTA closes its connections and shuts down. Depending on the amount of email traffic present, shutdown should take a few minutes.

2. **Resolve whatever problem exists with the channel or IMTA.**

3. **Click the IMTA pull-down menu and select Start IMTA.**

   The IMTA re-establishes its connections and starts up. Startup should take a few minutes.

▼ To Restart the IMTA

Command: `imta-restart`

AdminConsole>IMTA>IMTA pulldown>Restart IMTA

1. **From the IMTA property book, click the IMTA menu.**

2. **Choose Restart IMTA.**

   The IMTA and all channels restart. This operation takes a few minutes.

Backing Up and Restoring the IMTA Configuration

After the SIMS is installed, the server saves, or *backs up*, the IMTA, the Sun Message Store, and the directory service configuration. This configuration version is known as the *default configuration*. Subsequently, you can back up the latest IMTA configuration (also called the *current configuration*) at any time. The saved configuration is known as the *backup configuration*. Doing a backup overwrites the existing backup.

If for some reason you wish to use a previous configuration, you can restore one of the following configuration versions:

- Default configuration
- Backup configuration (provided that this exists)

▼ To BackUp and Restore the IMTA Configuration

AdminConsole>IMTA>IMTA pulldown>Save Current Config

1. **In the IMTA property book, click the IMTA pull-down menu and choose Save Current Config.**

   The current configuration is backed up.

2. **To restore a previous configuration, click the IMTA pull-down menu and choose Restore Default Config or Restore Backup Config, depending on which you prefer.**

   The backup configuration is restored.

Monitoring Channel Status

All channels can be monitored by SIMS. This feature can be helpful in diagnosing various problems.

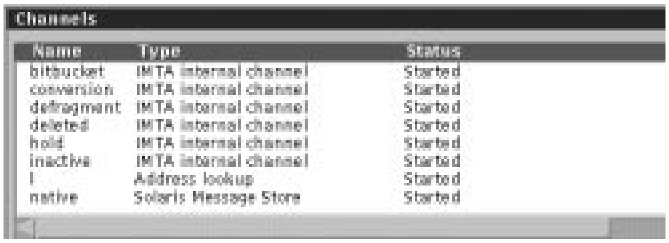
▼ To Monitor Channel Status

AdminConsole>IMTA>Channels

1. **Bring up the IMTA property book.**

2. **Click Channels from the Sections list.**

   The Channels section appears, as shown in FIGURE 5-2.



Channels

Name	Type	Status
bitbucket	IMTA internal channel	Started
conversion	IMTA internal channel	Started
defragment	IMTA internal channel	Started
deleted	IMTA internal channel	Started
hold	IMTA internal channel	Started
inactive	IMTA internal channel	Started
l	Address lookup	Started
native	Solaris Message Store	Started

FIGURE 5-2 Channels Section

The section displays a list of installed channels and channels that you created.

Alternative Delivery Programs

Users might want incoming mail passed to a program instead of to their mailbox. For example, users might want their incoming mail sent to a mail sorting program or to an autoreply agent like Vacation Notice. These alternative delivery programs can added to delivery options (see "Optional: Enable the delivery of email to UNIX programs by clicking the Program check box." on page 47) by using the `imta program` command (see "To Modify a User Entry" on page 41, Step 7). Alternative delivery programs must, however, conform to the following exit code and command- line argument restrictions:

Exit codes: If the subprocess exits with an exit code of 0 (`EX_OK`), the message is presumed to have been delivered successfully and is removed from IMTA's queues. If it exits with an exit code of 71, 74, 75, or 79 (`EX_OSERR`, `EX_IOERR`, `EX_TEMPFAIL`, or `EX_DB`), a temporary error is presumed to have occurred, and delivery of the message is deferred. If any other exit code is returned, then the message will be returned to its originator as undeliverable. These exit codes are defined in the system header file `/usr/include/sysexits.h`.

Command Line Arguments: Delivery programs can have any number of fixed arguments as well as the variable argument, `%s`, representing the user name for programs executed by the user or *username+domain* for programs executed by the postmaster, "inetmail." For example, the following command line delivers a recipient's mail using the program `procmail`:

```
/usr/lib/procmail -d %s
```

▼ To Make Delivery Programs Available to Users

Command: `imta-program`

These procedures add a delivery program to the User Profile described in "Optional: Enable the delivery of email to UNIX programs by clicking the Program check box." on page 47.

1. **Obtain delivery program executable.**

   The program must conform to the format specified in "Alternative Delivery Programs" on page 86.

2. **Create a symbolic link from the actual executable to `/opt/SUNWmail/imta/programs`**

   Make sure the actual executable has execute permissions for "`others`."

3. **Use the `imta program -a` command to add a new delivery program option.**

   Run `imta program` as root or inetmail (see *man page* for details). The format is as follows:

   ```
   imta program -a -m method_name -p program_name [ -g
   argument_list ] [ -e execute_permission ]
   ```

   Whether a program’s `execute_permission` must be “user” or “postmaster” depends on the program itself.

   a. **Examples:**

      Add a delivery program called `procmail1`, which executes the program `procmail` in the programs directory. Use the argument `-d username`, and make this program execute as the user. Use the `-e user` argument so that this option is available only to mail users with UNIX accounts:

      ```
      % imta program -a -m procmail1 -p procmail -g “-d %s” -e user
      ```

      Add a delivery program `print_hickory`, which executes the program `lp` with the arguments `-d hickory`. Make this program option available to all mail users.

      ```
      % imta program -a -m print_hickory -p lp -g “-d hickory”
      ```

Alias Synchronization Schedule

Rather than performing a directory query for each message that it processes, the IMTA caches directory information that is needed for processing a message. The directory information stored in the directory database is continuously updated. As a result, the directory information in the IMTA-directory cache must be synchronized periodically with the directory information in the directory service. This is called a *alias synchronization* or *dirsync* (directory cache synchronization) and can be done with the `imta-dirsync` command or it can be set up automatically on the Admin Console. (Note that the cache persists and is updated through an incremental or full dirsync.)

The IMTA supports full and incremental synchronizations.

- Full synchronization – The existing cache is replaced with a new cache completely rebuilt from information in the directory. After the synchronization occurs, the IMTA configuration file is rebuilt and then the IMTA is automatically restarted.

- Incremental synchronization – The existing cache is updated with user and group entries that were created or modified since the last full or incremental synchronization. The IMTA is not restarted.

  Specifically, during an incremental synchronization, the directory information in the cache is updated with:

  - User entries – New user entries and modifications to existing user entries. The cache is not updated with deleted user entries.
  - Group entries – New and deleted members of existing distribution lists and new distribution lists. The cache is not updated with deleted distribution lists or new rules for existing distribution lists. The new distribution list is also updated.

Note – Important! You must schedule each IMTA-directory cache in your mail system (master and replicas) to be fully or incrementally resynchronized at the same time. Not doing so could cause routing loops to occur.

Cache Synchronization Schedule Planning

By default, the IMTA-directory cache is fully synchronized every day at 2:00 am and incrementally synchronized every ten minutes.

The Admin Console enables you to reconfigure the synchronization schedule. Before reconfiguring this schedule, you must consider the following:

- A full synchronization requires that the IMTA be restarted, an operation that is performed automatically. Since restarting the IMTA is a CPU-intensive operation and will temporarily affect the overall mail server performance, Sun recommends scheduling full synchronizations at times when you anticipate that the mail server load is light, for example, during lunch hour or in the middle of the night.
- An incremental synchronization does not burden the CPU to the degree that a full synchronization does; in fact, the more often incremental synchronizations are performed, the less it burdens the CPU. However, an incremental synchronization does use CPU cycles and you do not want to schedule this operation more than necessary.

Depending on the number of users (mailboxes) your mail server services, scheduling one to six full synchronizations per day and incremental synchronizations every 5 to 30 minutes is sufficient.

▼ To Reconfigure the Alias Synchronization Schedule

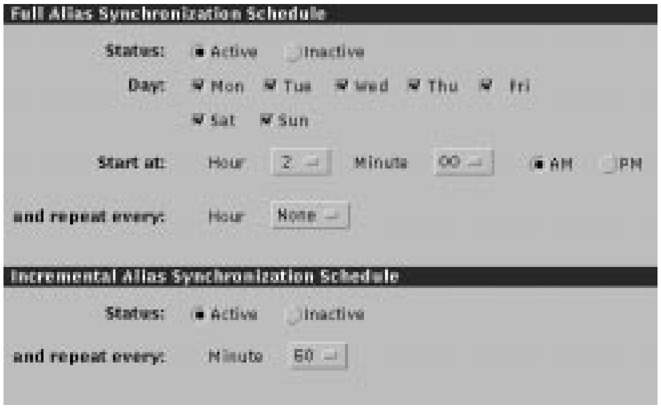
Command: `imta-dirsync`

AdminConsole>IMTA>Full Alias Synchronization (also Incremental Alias Synchronization)

1. **Click the IMTA icon on the Admin Console home page to bring up the IMTA property book.**

2. **From the Sections list, click Full Alias Synchronization Schedule.**

   The Full Alias Synchronization Schedule section appears followed by the Incremental Alias Synchronization Schedule section as shown in FIGURE 5-3.



Full Alias Synchronization Schedule

Status: ● Active ○ Inactive

Day: ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat ☑ Sun

Start at: Hour 2 Minute 00 ● AM ○ PM

and repeat every: Hour None

Incremental Alias Synchronization Schedule

Status: ● Active ○ Inactive

and repeat every: Minute 60

FIGURE 5-3 Schedule for Synchronizing Aliases Section

3. **Configure the full synchronization schedule.**

   a. **Click the Active button in the Status field to enable full synchronization.**

   b. **Click the days on which you want full synchronization to occur.**

   c. **Specify the time at which you want the first full synchronization to occur.**

   d. **If you want multiple full synchronizations to occur per day, use the menu to specify how often the synchronizations should occur.**

   For example, if you specify that full synchronizations should occur every four hours, then they will occur six times per day.

4. **Configure the Incremental Alias Synchronization Schedule.**

   a. **Enable incremental synchronization by clicking the Active button.**

b. Specify how often the incremental synchronization should occur.

▼ To Disable Full and Incremental Synchronization

AdminConsole>IMTA>Full Alias Synchronization (or Incremental Alias Synchronization)>Inactive

1. **Access the IMTA property book by clicking the IMTA icon on the home page.**
2. **Click on Full Synchronization Schedule.**
3. **Click the Inactive radio button in the full or incremental synchronization section.**
4. **Click the Apply button.**

IMTA Location Relative to Public Internet

If the IMTA is directly connected to the public Internet (such as on a firewall system), it delivers outbound mail by using the domain part (right-hand side) of the envelope recipient in the DNS and routes accordingly. Conversely, if the IMTA is not connected to the public Internet, outbound mail for external addresses has to be forwarded to a smart host—an SMTP host that can resolve addresses that the current IMTA cannot resolve.

This section describes how to specify the position of the IMTA relative to the public Internet, and how to specify a fully qualified smart host name if the IMTA is not directly connected to the Internet. The routing configuration will differ depending on whether the IMTA is or is not connected to the Internet. Depending on the position you select, the Admin Server will modify the IMTA rewrite rules to reflect that position.

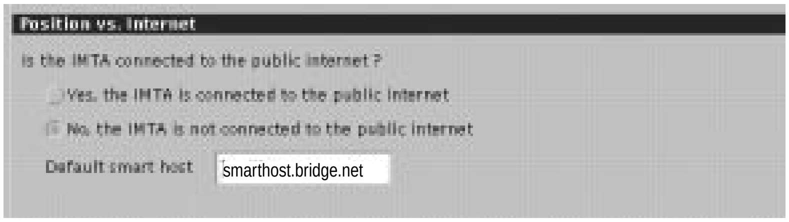
Note – Use this option only when the IMTA location relative to the public Internet changes. If the IMTA is connected to the Internet, but you want it to forward outbound mail to a dedicated outbound system, create an additional SMTP router channel to forward mail to this machine, then edit the configuration file `imta.cnf` to make the "." rule point to the newly created channel. See *SIMS Reference Guide* for more details.

▼ To Configure IMTA Position Relative to the Internet

AdminConsole>IMTA>Position Vs. Internet

1. **From the Sections list of the IMTA property book, click the Position Vs. Internet.**

   The Position versus Internet section appears as shown in FIGURE 5-4.



Position vs. Internet

Is the IMTA connected to the public internet ?

○ Yes, the IMTA is connected to the public internet

● No, the IMTA is not connected to the public internet

Default smart host: smarthost.bridge.net

FIGURE 5-4 Position versus Internet Section

2. **Determine whether the IMTA is connected directly to the public Internet.**

   If the IMTA is connected directly to the public internet, select Yes, the IMTA is connected to the public internet. If the IMTA is not directly connected to the public internet, click No, the IMTA is not connected to the Internet.

3. **If you indicated that the IMTA is not directly connected to the Internet, then specify the smart host name.**

   It must be a fully-qualified name. The syntax is `mailhost.domain`. Enter the name using ASCII characters. The characters are case-sensitive.

4. **Click the Apply button.**

Routability Scope

By default, the IMTA is expected to be able to resolve an address of the form `user@xzy.com`, where `xzy.com` is the mail domain name. To resolve addresses, the IMTA constructs an alias cache containing *all* users in the domain `xzy.com` via alias synchronization.

It might be useful to change the routability scope of the alias cache in the following cases:

- When the directory is not populated with the entire domain.
- To limit the size of the alias cache.
- To enforce routing policies. For example, if all mail going outside of the domain must be forwarded by a specific set of IMTAs.

The routability scope is the group of addresses to which the IMTA can route directly (send directly to the user's delivery mail store) or to which it can deliver locally.

This section explains how to set the routability scope to one of the following:

- Mail Server domains - This is the default scope for the IMTA. The IMTA is responsible for everyone in all the domains in the directory for which this IMTA is the mail host.
- Nobody – Indicates that the mail server does not support a user community. This setup is typical if your mail server is a backbone IMTA that routes messages between domains. It does not know of each mail user, but uses the host or domain specifications to forward the message to the appropriate mail server for delivery. For example, if a message is sent to *user*`@eng.stream.com`, the IMTA knows to forward this message to `mailhost.eng.stream.com`. Similarly, it can forward a message addressed to *user*`@qa.eng.stream.com` to `mailhost.qa.eng.stream.com`.
- Local system users only – The IMTA can deliver messages to local users only. The IMTA cannot deliver to nonlocal users. If a message arrives that is not addressed to a local user (that is, a user whose message store is on this particular server), the IMTA forwards it to a specified smart host without doing an alias table lookup.

Note – This option is supported for non-hosted domains only.

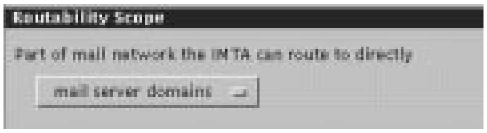
Modifying the routability scope modifies the way the IMTA persistent alias cache is created and modifies the IMTA rewrite rules.

▼ To Configure Routability Scope

AdminConsole>IMTA>Routability Scope

1. **From the Sections list of the IMTA property book, click Routability Scope.**

   The Routability Scope section appears as shown in FIGURE 5-5.



Routability Scope

Part of mail network the IMTA can route to directly

mail server domains

FIGURE 5-5 Routability Scope Section

2. **Select the portion of the mail network to which the IMTA can route using the pull-down menu.**

   The choices are *nobody*, *local system users only*, and *mail server domains*.

3. **If you selected the Mail Server Domains option, then make certain that mail server domains are configured.**

4. **Click the Apply button.**

Channels

The Channels section enables you to view the status of the IMTA channels. For more information, refer to “Monitoring Channel Status” on page 85. In addition, you can modify the properties of specific channels by double-clicking on the desired channel and bringing up the property book associated with that channel.

Configuring Channels

This section describes how to configure channel attributes. The IMTA includes the following configurable channels:

- Internet SMTP channel
- Intranet SMTP channel
- Router SMTP channel
- Sun Message Store channel
- `/var/mail` channel
- Pipe channel
- Deleted channel
- Inactive channel
- Hold channel

You can also add new channels as needed. Note that the number of SMTP channels will depend on the mail server’s position versus the Internet.

Channel configuration can also be done by editing the `imta.cnf` file. Editing the file allows you to add channel keywords that are not supported by the Admin Console. Refer to channels section in the *SIMS Reference Manual* (IMTA Configuration Chapter). Use extreme care when editing the configuration file as errors could result in IMTA malfunction.

Note – SIMS does not support the configuration of the UNIX to UNIX Copy Program (UUCP) channel using the Admin Console. You can configure the UUCP channel by editing the `imta.cnf` file. For more information on `imta.cnf`, refer to the *SIMS Reference Manual*.

TABLE 5-2 summarizes the configurable attributes of these channels, specifically which channels to which each attribute applies.

TABLE 5-2 Configuring Channels

Configurable Aspect	Channel Applies To	Description
Channel description	Applies to all channels	You can generate a description of a channel for administrative purposes only.
Router	Applies only to SMTP router channels	In the event that an IMTA cannot resolve a particular message address, you must configure a host to which the IMTA can route the message.
Character set labels	All channels	Determines the label for 7-bit character sets and for 8-bit character sets to be used in plain text messages.
Message Limitation	Some attributes apply to SMTP channels only	Determines how the channels handle large messages and messages with many recipients.
Delivery Status Notification	Applies to all channels	Determines how a channel handles the messages that warn of or return undelivered mail.
Report Problems to Postmaster	Applies to all channels	Determines how a channel handles the sending of warning messages to the postmaster.
Diagnostics Output	Applies to all channels	Determines whether a channel produces diagnostic output for its master program, slave program, or both.
Performance Tuning	Applies to all channels	Determines how the IMTA delivers messages and defers the processing of messages, thereby tuning its performance.
Logging	Applies to all channels	When selected, provides logging information to the global log.
Multiple Internet Mail Extensions (MIME) Fragmentation	Further applies to Sun Message Store, `/var/mail`, and pipe channels only.	You can enable a channel to reassemble message fragments into one message upon receipt.
Rewrite rules	Applies to all channels	You can add a new rewrite rule to an existing or newly created channel, or delete or modify an existing rewrite rule.

▼ To Create a Channel

You can create channels of the type *SMTP explicit router* only through the Admin Console. No limitations exist for the overall number of channels that you can create and the number of specific types of channel that you can create.

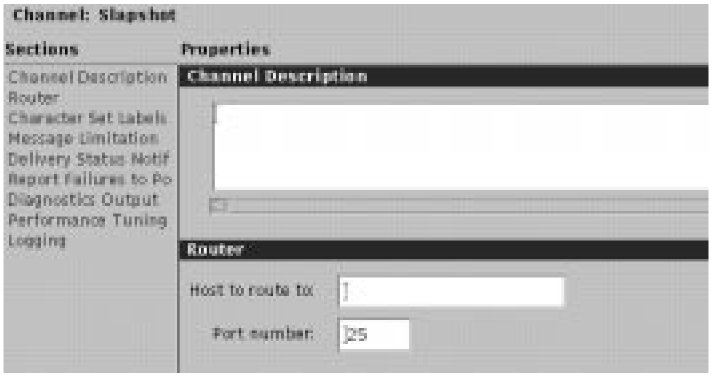
AdminConsole>IMTA>Create pulldown>Channel

1. **In the Admin Console home page, click IMTA.**
2. **In the IMTA property book, choose Channel from the Create menu.**

   The Create Channel dialog box appears.
3. **Enter a name for your new channel.**

   Valid entries include ASCII characters. A maximum of 40 characters is accepted.
4. **Click the OK.**

   The New Channel Property Book appears. Note that this is similar to the Existing Channel Property Book described in "To Access a Channel's Property Book" on page 97.



Channel: Slapshot

Host to route to:

Port number: 25

FIGURE 5-6 New Channel Property Book

5. **Fill in the various sections and press OK**

   Only two sections are mandatory at this time: Router and Message Limitation. Enter the *Host to route to* field and change the *Max. no. of recipients per msg* field from 0 to whatever maximum number of recipients you wish to allow a single message to be sent by the IMTA. If you don't change this value, the channel will not work. The remaining fields can be entered at a later time. These fields are described in the remaining sections of this chapter.

6. **After the channel is created, you must configure rewrite rules for the new channel to process messages properly.**

   Refer to “Configuring Channels” on page 94 and “Rewrite Rules” on page 109 for more information on rewrite rules and configuring the channel.

To Delete a Channel

You can delete the router SMTP channel (explicit route) that you created.

```
AdminConsole>IMTA>Channels>Selected pulldown>Delete Channel
```

1. **In the IMTA property book, click Channels in the Sections list.**

   The Channels section appears. This section displays a list of installed channels.

2. **Click the channel that you want to delete.**

   The channel you want to delete is highlighted.

3. **Choose Delete Channel from the Selected menu.**

   Confirm that you want to delete the channel.

4. **Click the Yes button.**

   The deleted channel name, type, and status are removed from the channel list.

To Access a Channel’s Property Book

```
AdminConsole>IMTA>Channels
```

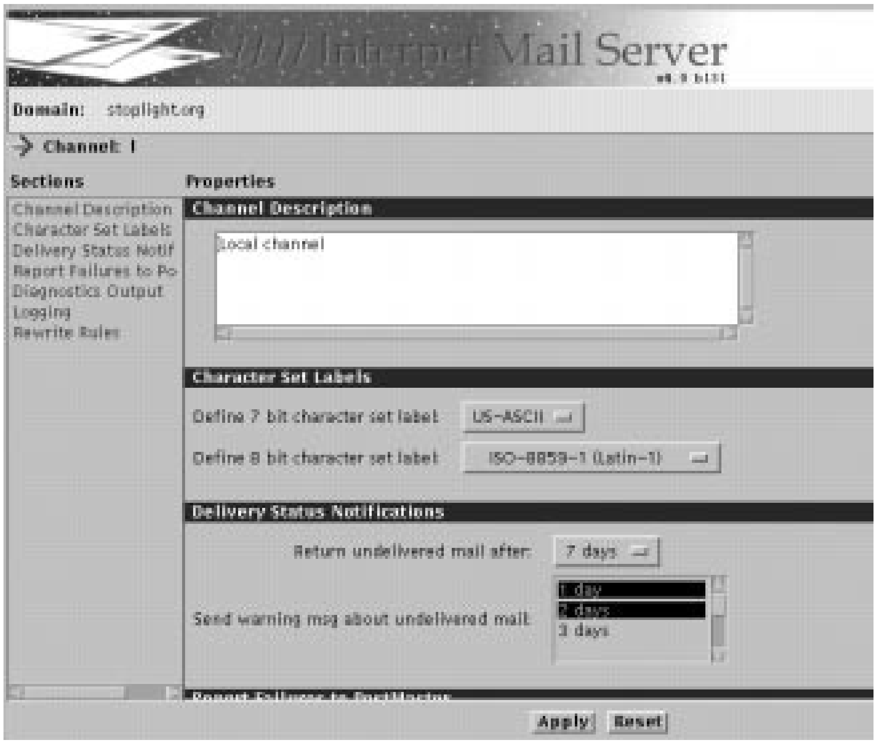
1. **In the Admin Console home page, click the IMTA icon.**

2. **In the Sections list, click Channels.**

   The Channels section appears. This section displays a list of channels.

3. **Either click the desired channel in the list and then select Properties from the Selected menu, or double-click the desired channel in the list.**

   The channel property book appears, as shown in FIGURE 5-7.



Domain: stoplight.org

Channel: l

Channel Description

Local channel

Character Set Labels

Define 7 bit character set label: US-ASCII

Define 8 bit character set label: ISO-8859-1 (Latin-1)

Delivery Status Notifications

Return undelivered mail after: 7 days

Send warning msg about undelivered mail: 1 day, 2 days, 3 days

FIGURE 5-7 Sample Channel Property Book

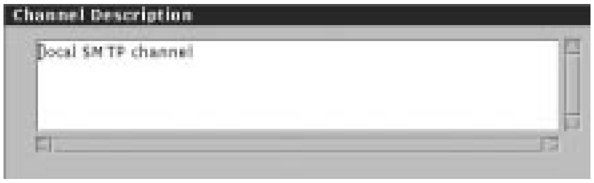
▼ To Configure a Channel Description

By default, the IMTA generates a channel description. You can update this description with any desired notes or details. This description is for administrative purposes only and does not affect the behavior of the channel.

AdminConsole>IMTA>Channels>double-click desired channel>Channel Description

1. **Click Channel Description from the Sections list of the channel property book.**

   See “To Access a Channel’s Property Book” on page 97 for more information. The Channel Description section appears, as shown in FIGURE 5-8.



Local SMTP channel

FIGURE 5-8 Channel Description Section

2. **Update the text description of the channel with up to 256 characters.**
3. **Click the Apply button.**

▼ To Configure a Router Host

Note – This section applies to SMTP router channels only.

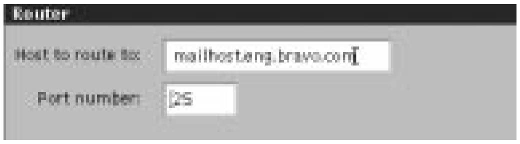
In order to route messages to a particular domain, the IMTA may rely on the DNS and deliver mail through the SMTP intranet/SMTP Internet channels. An alternative is to specify the domain host to which to route mail. The messages are then delivered through an SMTP router channel

Note that if the IMTA is not connected to the Internet, mail to all external domains is forwarded to a smart host by the default SMTP router channel. The smart host is the host to route to for the default SMTP router channel.

AdminConsole>IMTA>Channels>selected channel>Selected Menu>Properties>Router

1. **From the Sections list of the Channel property book, click Router.**

   To find out how to access the channel property book, see “To Access a Channel’s Property Book” on page 97. The Router section appears as shown in FIGURE 5-9.



Host to route to: mailhost.eng.bravo.com

Port number: 25

FIGURE 5-9 Router Section

2. **Type the host name of the IMTA that functions as a router using the following syntax:**

   hostname.domain

   A sample host name is `mailhost.eng.bravo.com`. Be sure to enter the fully qualified name of the smarthost.

3. **Type the port number through which the routed messages should enter.**

4. **Click the OK button.**

   You are prompted to restart the IMTA.

5. **Click the Yes button.**

▼ To Configure Character Set Labels

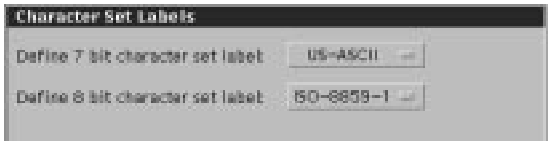
The MIME standard provides a means of labeling or naming the character set used in a plain text message. The character set labels are inserted in the Content-type header of a message, indicating what type of characters are used in the message.

AdminConsole>IMTA>Channels>selected channel>Selected Menu>Properties

1. **In the Sections list of the Channel property book, click Character Set Labels.**

   To find out how to access the channel property book, see "To Access a Channel's Property Book" on page 97.

   The Character Set Labels section appears as shown in FIGURE 5-10.



Character Set Labels

Define 7 bit character set label: US-ASCII

Define 8 bit character set label: ISO-8859-1

FIGURE 5-10 Select Character Set Section

2. **Use the menus to specify a label for the 7-bit character set and for the 8-bit character set.**

3. **Click the Apply button.**

   A dialog box appears prompting you to restart the IMTA. click Yes.

Message Limitation

Some email systems and IMTAs encounter problems when handling large messages. You can control how the channels handle large messages (measured in bytes and number of lines) for the SMTP intranet/Internet channels, SMTP explicit route channels, and local or message store channels (for other channels, this feature has no effect). You can specify that messages be limited by size or number of recipients, or that they be fragmented if they exceed a certain size.

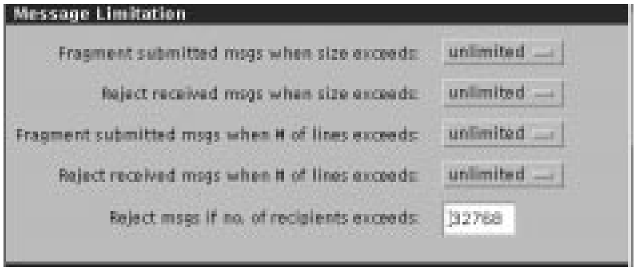
▼ To Configure Message Limitation

Utilities: `imadmin-modify-msglimits`
`imadmin-search-msglimits`

AdminConsole>IMTA>Channels>selected channel>Selected Menu>Properties>Message Limitation

1. **In the Sections list of the Channel property book (see "To Access a Channel's Property Book" on page 97), click Message Limitation.**

The Message Limitation section appears as shown in FIGURE 5-11.



Message Limitation

Fragment submitted msgs when size exceeds: unlimited

Reject received msgs when size exceeds: unlimited

Fragment submitted msgs when # of lines exceeds: unlimited

Reject received msgs when # of lines exceeds: unlimited

Reject msgs if no. of recipients exceeds: 32768

FIGURE 5-11 Message Limitation Section

To set local user to local user mail message limitations, configure the *local* (Solaris Message Store) or *message Store* (Sun Message Store) channel depending on the recipient's channel. Note that the *local* and *message Store* channels do not support either of the *Fragmented submitted msgs* parameters or the *Max. # of recipients per msg* parameter.

2. **(Optional) Set a limit on message size.**

3. **(Optional) Set a limit on the number of lines in incoming messages.**

You can specify a limit at which a message should be fragmented into smaller messages and a limit at which a message should be deemed too large and rejected. The default is unlimited.

4. **Set limits on the maximum number of recipients per message by typing a value.**

   Valid entries include 0 to 32,768. By default, a channel handles up to 32,268 recipients per message. If you prefer, specify a limit at which a message is deemed to have too many recipients and is rejected.

5. **Click the Apply button**

   You are prompted to restart the IMTA. Click Yes.

Delivery Status Notification

Occasionally, a channel may not be able to process an incoming message (for example, a remote MTA may go down, which is considered a transient failure, or a user is unknown, which is a permanent failure). When this happens, SIMS sends a delivery status notification or *notary message* to the postmaster and the sender.

For a permanent failure, the message is bounced and a notification is sent to the postmaster.

For a transient failure, by default, the channel will send up to three notary messages to the originator of the message at the following intervals: 1 day, 2 days, 4 days, and 7 days after the original message was sent. Each notary message will inform the originator that the original message is undeliverable, why the message is undeliverable, and how long delivery attempts will continue. By default, 12 days after the original message was sent, the original message will be returned to the originator. If the failure is corrected before the 12 days, the messages will be delivered. You can reconfigure the interval at which the notary messages are sent and the original message is returned.

▼ To Configure Delivery Status Notification

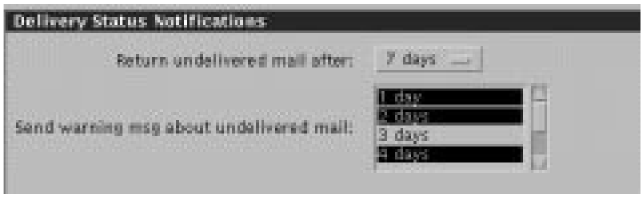
Utility(s): `imadmin-modify-notary` & `imadmin-search-notary`

AdminConsole>IMTA>Channels>selected channel>Selected Menu>Properties>Delivery Status Notification

This option is not supported for the SIMS Message Store Channel.

1. **In the Sections list of the Channel property book, click Delivery Status Notification.**

   The Delivery Status Notification section appears as shown in FIGURE 5-12.



Delivery Status Notifications

Return undelivered mail after: 7 days

Send warning msg about undelivered mail: 1 day, 2 days, 3 days, 4 days

FIGURE 5-12 Deliver Status Notification Section

2. **Configure the number of days after which undelivered mail should be returned.**
3. **Configure the interval and the days after which a message is sent that a notary message is sent.**

   Click up to four selections to specify intervals.
4. **Click the Apply button.**

   You are prompted to restart the IMTA.Click Yes.

Notary Message Locale

To change the default locale (`C`) so that *notary messages* (text messages sent by the IMTA to an email sender indicating delivery or nondelivery status of a sent message) appear in a different character set, you will need to create a separate locale directory under the IMTA configuration directory and edit `imta_tailor` file such that the `IMTA_LANG` points to the new locale directory.

▼ To Change the Notary Message Locale

For example, if you want the notary messages to appear in Japanese, do the following:

1. **Create a directory for the Japanese locale in `/etc/opt/SUNWmail/imta/locale`:**

   ```
   % mkdir /etc/opt/SUNWmail/imta/locale/ja
   ```
2. **Create a directory under the `ja` directory to hold the messages:**

   ```
   % mkdir /etc/opt/SUNWmail/imta/locale/ja/LC_MESSAGES
   ```

3. **Copy the nine message files from the `/etc/opt/SUNWmail/imta/locale/C/LC_MESSAGES` (default) directory into the `/etc/opt/SUNWmail/imta/locale/ja/LC_MESSAGES` directory.**

   The files are:

   ```
   return_bounced.txt    return_delivered.txt  return_prefix.txt
   return_deferred.txt   return_failed.txt     return_suffix.txt
   return_delayed.txt    return_forwarded.txt  return_timedout.txt
   ```

4. **Translate the message text in the files into the Japanese character set.**

   You may also wish to provide the message text in English as well as any other local languages for senders who do not speak Japanese.

5. **Edit the tailor file (`/etc/opt/SUNWmail/imta/imta_tailor`).**

   Change the line:

   ```
   IMTA_LANG=/etc/opt/SUNWmail/imta/locale/C/LC_MESSAGES
   ```

   to

   ```
   IMTA_LANG=/etc/opt/SUNWmail/imta/locale/ja/LC_MESSAGES
   ```

6. **Restart the IMTA.**

▼ To Configure Report Failures to the Postmaster

Utility: `imadmin-modify-postmaster`
`imadmin-search-postmaster`

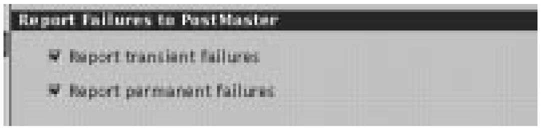
By default, the local postmaster receives a copy of all notary messages for transient and permanent failures except those undelivered messages that do not have an originator address. You can reconfigure the channel to send a copy of all or no notary messages to the local postmaster. Although receiving a copy of each of the notary messages may help you monitor the state of the channel queue, you will have to weigh this benefit against the increase in traffic that the channel will need to handle. To configure what part of the message is sent to the postmaster, you can add additional channel keywords in `imta.cnf` (see the *SIMS Reference Manual*).

AdminConsole>IMTA>Channels>selected channel>Selected Menu>Properties>Report Problems to Postmaster

1. **In the Sections list of the Channel property book, click Report Problems to Postmaster.**

   To find out how to access the channel property book, see “To Access a Channel’s Property Book” on page 97.

The Report Problems to Postmaster section appears as shown in FIGURE 5-13.



Report Failures to PostMaster

☑ Report transient failures

☑ Report permanent failures

FIGURE 5-13 Report Problems to Postmaster Section

2. **To send transient failure warning messages to the local postmaster, click Report transient failures.**

3. **To send warning messages of permanent failures to the local postmaster, click Report permanent problems.**

4. **Click the Apply button.**

   You are prompted to restart the IMTA. Click Yes.

Diagnostics Output

By default, a channel does not produce diagnostics output for its master and slave programs. You can reconfigure the channel so that it produces diagnostics output for either its master program, its slave program, or both.

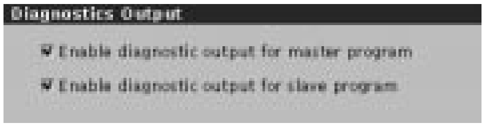
When enabled, diagnostic output is written to the log file associated with the channel program. For more information on diagnosis using log files refer to the *SIMS Reference Manual*.

▼ To Configure Diagnostics Output

AdminConsole>IMTA>Channels>selected channel>Selected Menu>Properties>Diagnostics Output

1. **In the Sections list of the Channel property book (see "To Access a Channel's Property Book" on page 97), click Diagnostics Output.**

The Diagnostics Output section appears as shown in FIGURE 5-14.



Diagnostics Output

☑ Enable diagnostic output for master program

☑ Enable diagnostic output for slave program

FIGURE 5-14 Diagnostics Output Section

2. **Determine whether diagnostic output is wanted.**

   - To generate diagnostic output for the channel's master or slave program, click the corresponding check box.

3. **Click the Apply button.**

   You are prompted to restart the IMTA. Click Yes. The debug output file is at `/var/opt/SUNWmail/imta/log/`.

   The format of the channel debug file name is as follows:

   `channel_master.log_xxxxxx` - master debug file (`xxxxx` is a random string).
   `channel_slave.log_xxxxxx` - slave debug file (`xxxxx` is a random string).

▼ To Set Recipient Limitation

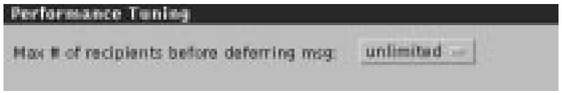
By default, the SMTP channel allows an unlimited number of recipients for a message without deferring processing. Too many recipient addresses can result in a delay in message processing. If the delay is long enough, network timeouts can occur and this in turn can lead to repeated message submission attempts and other problems. You can specify a limit of recipients for a single message at which message processing is deferred. When the specified number is exceeded, the message is enqueued and the remaining recipients are not verified on-line. Nondelivery receipts are generated for recipients later found undeliverable.

AdminConsole>IMTA>Channels>double-click channel>Properties>Performance Tuning

1. **In the Sections list of the Channel property book, click Performance Tuning.**

   See "To Access a Channel's Property Book" on page 97.

   The Performance Tuning section appears as shown in FIGURE 5-15.



Performance Tuning

Max # of recipients before deferring msg: unlimited

FIGURE 5-15 Performance Tuning Section

2. **Specify a limit of recipients for a single message using the menu.**
3. **Click the Apply button.**

Message Logging

By default, a channel logs in each message in `/var/opt/SUNWmail/imta/log/mail.log_current`. You can reconfigure the channel so that it logs in each message as it enters and is removed from the queue.

By default a log entry consists of the following fields:

- Date and time that entry was made
- Name of the source channel (channel that message originated from)
- Name of the destination channel (channel that message needs to be delivered to)
- Type of entry:
  - E = message was entered into the channel queue
  - D = message was removed from the channel queue
  - Q = an unsuccessful attempt was made to remove the message from the channel queue
- Size of the message in kilobytes
- Address in the From envelope after rewriting
- Address in the To header

For more information refer to **Chapter 12, “SIMS Monitoring and Logging** and to the *SIMS Reference Manual*.

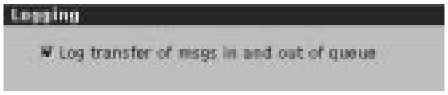
▼ To Configure Message Logging

AdminConsole>IMTA>Channels>double-click channel>Properties>Logging

1. **From the Sections list of the channel property book, click Logging.**

   To find out how to access the Channel property book, see "To Access a Channel's Property Book" on page 97.

   The Logging section appears as shown in FIGURE 5-16.



Logging

☑ Log transfer of msgs in and out of queue

FIGURE 5-16 Logging Section

2. **To enable the logging of each message as it enters and is removed from the channel queue, click the check box.**

3. **Click the Apply button.**

   You are prompted to restart the IMTA. Click Yes.

Reassembling MIME Messages

Note – This section applies to the UNIX to UNIX Copy Program (UUCP) channel, Sun Message Store channel, `/var/mail` channel, and pipe channel only.

Occasionally a large message must traverse email systems that impose message size limitations. MIME allows the breaking up of a large message into smaller messages, a process known as *fragmentation*. A Message/Partial Content-Type header field that appears in each of the smaller messages or *fragments* contains information that helps reassemble the fragments into one message, a process known as *defragmentation*.

By default, the Sun Message Store channel, `/var/mail` channel, and pipe channel do not defragment a message. You can configure each of these channels to reassemble a fragmented message upon receipt.

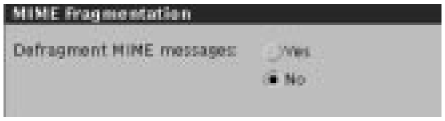
For complete information on message fragmentation and defragmentation, and the Message/Partial Content-Type header field, refer to RFC 1521.

▼ To Enable Reassembly of Message Fragments

AdminConsole>IMTA>Channels>double-click channel>Properties>MIME Fragmentation

1. **From the Sections list of the Channel property book, click MIME Fragmentation.**

   The MIME Fragmentation section appears as shown in FIGURE 5-17.



MIME Fragmentation

Defragment MIME messages: ○ Yes ● No

FIGURE 5-17 MIME Fragmentation Section

2. **Determine whether message fragments are reassembled.**
   - To enable the reassembly of message fragments, click Yes.
   - To disable the reassembly of messages, click No.

3. **Click the Apply button.**

   You are prompted to restart the IMTA. Click Yes.

Rewrite Rules

The Admin Console enables you to add or modify a rewrite rule for the following type of channel: SMTP Intranet, SMTP Internet, SMTP explicit route (i.e SMTP ROUTER), Address lookup (the LOCAL channel). If you want to add Rewrite rules for other channels, you need to modify the configuration files directly (see *SIMS Reference Manual*). The Admin Console also enables you to delete or modify an existing rewrite rule associated with an existing channel.

Before adding or modifying a rewrite rule for a particular channel, read the associated conceptual information in the *SIMS Concepts Guide* and *SIMS Reference Manual* (IMTA Configuration chapter). When adding or modifying a rewrite rule, you might need to configure the following elements:

- Pattern
- Domain template
- Element to which rule applies

- Address direction
- Order of rewrite rules

A pattern is a string composed of ASCII text, which might include wildcard characters that can potentially match the host/domain specification of an incoming email address. The host/domain specification is the portion that is to the right of the at (@) sign; for example, in the address `john.smith@eng.acme.com`, the host/domain specification of the address is `eng.acme.com`. The wild card character that you can specify is an asterisk (*). An example of a pattern entry is

```
*.acme.com
```

A domain template defines how the host/domain specification of the address is rewritten. A template can be composed of one or both of the following elements:

- A full static host/domain specification, for example, `corp.acme.com`, or a portion of a host/domain specification (a portion of the address tokens), for example, `.com`.
- A single field substitution string that dynamically rewrites one address token of the host/domain specification represented by a wild card character (*). The address token to be rewritten can be the portion of the address that did not match the rewrite rule pattern or the portion that matched the wild card character. The rewriting of a host/domain specification is based on the contents of the specification itself. The template can include multiple field substitution strings.

The syntax of the field substitution string is as follows:

`$&`*`n`*

where *n* is an integer from 0 to infinity. The integer *n* represents the unmatched or wild card address token that is to be rewritten. From left to right, the leftmost address token is represented by the integer 0; the second from the left is represented by the integer 1, and so on. An example of a template entry is

```
$&0.$&1.com
```

The element that the rewrite rule applies to determines if the rule applies to the address that appears on the envelope only, the message header only, or both.

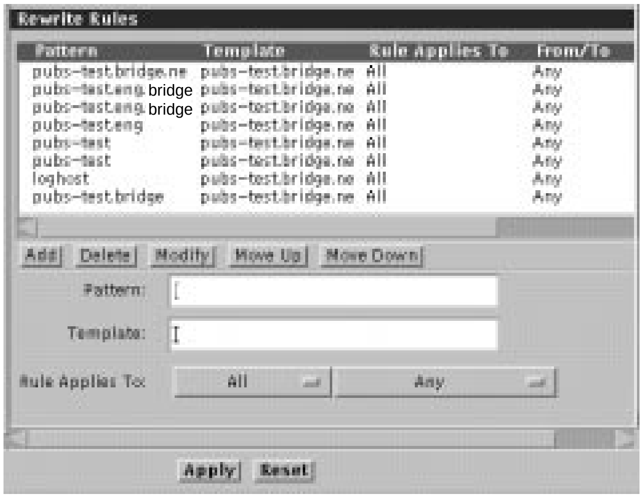
Address direction determines whether the rewrite rule applies to a forward address (`To`, `CC`, and `BCC` headers + envelope `RCPT TO:`) or a backward address (From or Reply-to headers + envelope `FROM:`).

▼ To Add, Delete, or Modify a Rewrite Rule

AdminConsole>IMTA>Channels>double-click channel>Properties>Rewrite Rules

1. **In the Sections list of the Channel property book (see “To Access a Channel’s Property Book” on page 97, click Rewrite Rules.**

   FIGURE 5-18 shows the Rewrite Rules section.



Rewrite Rules

Pattern	Template	Rule Applies To	From/To
pubs-test.bridge.ne	pubs-test.bridge.ne	All	Any
pubs-test.eng.bridge	pubs-test.bridge.ne	All	Any
pubs-test.eng.bridge	pubs-test.bridge.ne	All	Any
pubs-test.eng	pubs-test.bridge.ne	All	Any
pubs-test	pubs-test.bridge.ne	All	Any
pubs-test	pubs-test.bridge.ne	All	Any
loghost	pubs-test.bridge.ne	All	Any
pubs-test.bridge	pubs-test.bridge.ne	All	Any

Pattern:

Template:

Rule Applies To: All Any

FIGURE 5-18 Rewrite Rules Section

   The Rewrite Rules section is divided into two sections: a display of already existing rewrite rules in the top part of the display and various configurable fields in the bottom part of the display.

2. **If you want to delete, modify, move up, or move down an existing rule in the display, click the rule in the top part of the display to highlight it.**

   The bottom part of the display shows the existing entries for pattern and template as well as the settings for protocol and direction.

3. **Take one of the following actions with the existing rewrite rule:**

   a. **Delete the rule.**

      Click the Delete button.

   b. **Modify the rule.**

      Delete and reenter the Pattern and Template entries and use the pull-down menus to reselect the value for Rules Applies to and Address. Click the Modify button.

   c. **Move the rule up or down in the list of rules.**

      Click either the Move Up or Move Down button.

4. **If you prefer, add a new rewrite rule using the following steps:**

a. **Specify a pattern.**

   Enter a pattern composed of ASCII text and the wild card character of an asterisk (*). An example of a pattern entry is

   `*.acme.com`

b. **Specify a template.**

   Enter either a full host/domain address, for example, `corp.acme.com`, or a partial host/domain address set off by decimals, for example, `.com`.

   If you enter a partial host/domain address, you also need to specify the appropriate number of field substitution strings. The syntax of the field substitution string is as follows:

   `$&`*`n`*

   where *n* is an integer from 0 to infinity. The integer represents the address token that is to be rewritten. From left to right, the leftmost address token is represented by the integer 0; the second from the left is represented by the integer 1, and so on. For example, if an incoming address matches the following rewrite rule pattern:

   `*.acme.com`

   then the domain template will consist of the following:

   `$&0.acme.com`

c. **Specify whether you want the rewrite rule to apply to envelope, message header, or both, using the** *All* **pull-down menu.**

d. **Specify whether you want the rewrite rule to apply to** *RCPT To, CC, Bcc, ...***, or** *MAIL From, Apply-to, ...* **or both using the** *Any* **pull-down menu.**

e. **Click the Add button.**

5. **Click the Apple button.**

   You are prompted to restart the IMTA. Click Yes.

Monitoring Channel Queues

Utilities: `imta-counters`, `immonitor-queue`,

SMTP command: `xsta` (allows you to get current channel counters without having to log into the system.

You can monitor accumulated message traffic statistics for each IMTA channel queue (includes user-created channels). At the same time, you can compare statistics accumulated for one channel queue to statistics accumulated for the IMTA.

The queue monitor accumulates the following statistics:

- Received messages – Number of messages that have entered the channel queue
- Submitted messages – Number of messages that have exited from one channel queue and entered another channel queue
- Delivered messages – Number of messages that have exited the channel queue
- Stored messages – Number of messages currently stored in the channel queue
- Received volume – Volume of messages that have entered the channel queue measured in kilobytes
- Submitted volume – Volume of messages that have exited from the channel queue and entered another channel queue measured in kilobytes
- Delivered volume – Volume of messages that have exited from the channel queue measured in kilobytes
- Stored volume – Volume of messages currently stored in the channel queue measured in kilobytes

For more information refer to “Snapshot of Message Traffic Through IMTA” on page 144.

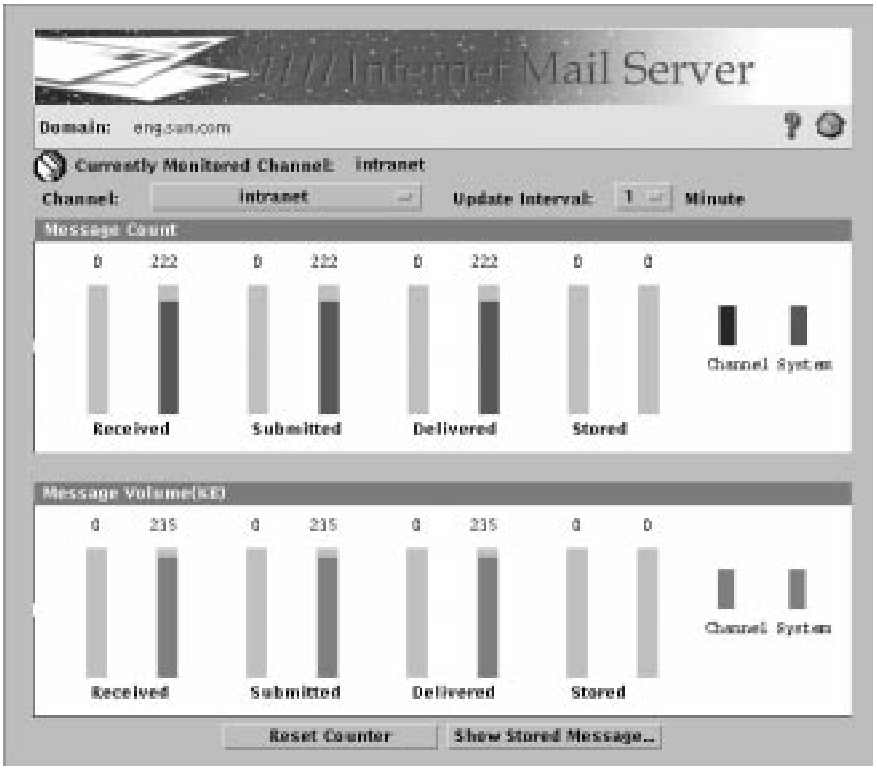
▼ To Monitor the IMTA Channel Queues on Admin Console

AdminConsole>IMTA>Channels>select channel>Selected pulldown>Monitor Queue

1. **From the Admin Console home page, click the IMTA icon.**
2. **Click Channels from the Sections list.**
3. **Click the channel whose queue you want to monitor.**

   The channel name, type, and status are highlighted.
4. **Choose Monitor Queue from the Selected pull-down menu.**

   The Monitoring Queue page for the selected channel appears (FIGURE 5-19).



Domain: eng.sun.com

Currently Monitored Channel: intranet

Channel: intranet

Update Interval: 1 Minute

FIGURE 5-19 Internet Message Transfer Agent Channel Queue Monitor

The queue monitor incorporates the following color codes:

- Red – Message count per channel
- Blue – Message count per system
- Red – Message volume per channel
- Blue – Message volume per system

5. **(Optional) Change the time interval in which data is polled.**

   Click the Update Interval option pull-down menu and select the desired option.

6. **(Optional) Reset the counter by clicking the Reset Counter button.**

   Note that after resetting the counter, messages in transit will not be counted; therefore, the statistics provided in the Message Count portion of the page will not be accurate. In this situation, rely on the statistics presented in the Message Volume portion of the page.

7. **To view statistics for other channel queues, click the Channel option pull-down menu and select the desired channel.**

   This list of channels includes all installed and user-created channels.

▼ To Monitor the IMTA Channel Queues Using xsta

SMTP command: `xsta`

The advantage of this command for monitoring channel queues is that you can get current channel counters without having to log into the system. Simply telnet to port 25 on a mail server and enter `xsta`.

CODE EXAMPLE 5-1 xstra Command Output (shortened)

```
$ telnet 25 mailserver
connecting to host mailserver (129.146.84.66), port 25
connection open
220 mailserver.eng.bridge.com -- Server ESMTP (Sun Internet Mail Server
sims.4.0.1998.10.14.10.04) xsta
250-2.3.0 Channel                     Messages  Recipients      Blocks
250-2.3.0 ------------------------  ----------  ----------  ----------
250-2.3.0 l
250-2.3.0     Received                       0         0         0
250-2.3.0     Stored                         0         0         0
250-2.3.0     Delivered                      0         0         0 (0 first time)
250-2.3.0     Submitted                    123       123       124
250-2.3.0     Failed                         0         0         0
250-2.3.0
250-2.3.0 native
250-2.3.0     Received                     127       127       136
250-2.3.0     Stored                         0         0         0
250-2.3.0     Delivered                   145       145       154 (145 first time)
250-2.3.0     Submitted                      0         0         0
250-2.3.0     Failed                         0         0         0
250-2.3.0
250-2.3.0     Queue time/count          102619/145 = 707.717
250-2.3.0     Queue first time/count    102619/145 = 707.717
...
```

Viewing Enqueued Messages

You can also view a listing of the messages currently in the channel queue. The messages are stored for various reasons; for example, the mail server may be currently unavailable and the message delivery will be retried later. The type of information you can view about the stored messages includes the following:

- Message ID
- Message originator
- Date / time that message was originated
- Message size
- Contents of message itself

Once you find the specific message, you can view the contents of the message, save it, or delete it from the queue.

▼ To View Messages Stored In the IMTA Channel Queues

AdminConsole>IMTA>Channels>selected channel>Selected Menu>Monitor Queue>Show Stored Message

1. **From the Admin Console home page, click the IMTA icon.**

   The IMTA property book appears.

2. **From the Sections list, click Channels.**

   The Channels section appears.

3. **Click the channel whose queue you want to monitor.**

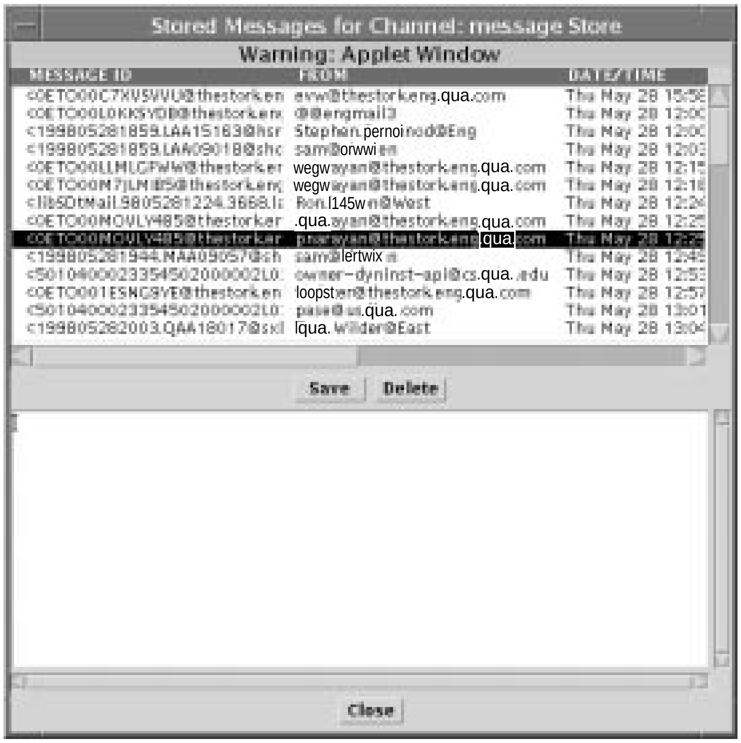
   The channel name, type, and status is highlighted.

4. **Click the Selected pull-down menu and select Monitor Queue.**

   The Monitoring Queue page with statistics for the selected channel appears.

5. **From the Monitoring Queue page, click the Show Stored Message button.**

   The Stored Messages dialog appears as shown in FIGURE 5-20.



MESSAGE ID	FROM	DATE/TIME
<OETO00C7XV5VVU@thestork.en	evw@thestork.eng.qua.com	Thu May 28 15:58
<OETO00L0KK5YDB@thestork.en	@@engmail3	Thu May 28 12:00
<199805281859.LAA15163@hsr	Stephen.pernoinod@Eng	Thu May 28 12:00
<199805281859.LAA09018@shc	sam@orwwien	Thu May 28 12:03
<OETO00LLMLGFWW@thestork.er	wegwayan@thestork.eng.qua.com	Thu May 28 12:15
<OETO00M7JLM85@thestork.eng	wegwayan@thestork.eng.qua.com	Thu May 28 12:18
<libSDtMail.9805281224.3668.l	Ron.l145wn@West	Thu May 28 12:24
<OETO00MOVLY485@thestork.er	.qua.ayan@thestork.eng.qua.com	Thu May 28 12:25
<OETO00MOVLY485@thestork.er	pnarayan@thestork.eng.qua.com	Thu May 28 12:2
<199805281944.MAA09057@sh	sam@lertwix.n	Thu May 28 12:45
<50104000233545020000002L0	owner-dyninst-api@cs.qua.edu	Thu May 28 12:53
<OETO001ESNG9VE@thestork.en	loopster@thestork.eng.qua.com	Thu May 28 12:57
<50104000233545020000002L0	pase@us.qua.com	Thu May 28 13:01
<199805282003.QAA18017@sxl	lqua.Wilder@East	Thu May 28 13:04

FIGURE 5-20 Stored Queue Monitoring

   A listing of stored messages appears in the top half of the dialog.

6. **(Optional) View the contents of the message by double-clicking the message in the list.**

   The contents of the message displays in the bottom half of the page.

7. **(Optional) Save or delete a message from the channel queue.**

   Click the message and then click the Save or Delete button as appropriate.

8. **Close the Stored Messages dialog by clicking the Close button.**

DNS-based Canonicalization

Note – DNS-based canonicalization will only work in the default domain and its subdomains.

Canonicalization is the process of converting an aliased or shortened domain name to its fully qualified domain name (FQDN) or *canonical* domain name. A fully qualified email address has the following forms:

`<uid>@<mailhost>.<company name>.com` (example: ed@rocket.stream.com)

`<uid>@<subdomains>.<company name>.com` (example: al@corp.bridge.com)

There are two primary reasons why domain canonicalization is needed: 1) allowing the short address form to be used within a domain, 2) to canonicalize the FROM: address such that return mail has a deliverable address.

Example for reason 1: You may wish to set up your email system such that users within the same domain can send mail to each other by entering a short form of the address without the FQDN. Thus, if a domain is `corp.bridge.com` and your server name is `hourglass`, you may want to provide users with the ability to send local mail using the form `<uid>@hourglass` or `<uid>@hourglass.corp` or `<uid>@corp` instead of `<uid>@corp.bridge.com`.

Example for reason 2: Some email clients in your system may be set up such that the FROM: header appends the short form of the user's email address. If a recipient wants to reply to the sender, a short form return address, for example `uid@corp`, is useless since a fully qualified address is needed to complete a delivery. For this reason, address canonicalization should be done as early in the delivery process as possible.

Address canonicalization must perform two tasks:

1. Qualify non-fully-qualified domain names:

   ```
   <uid>@mailhost --> <uid>@mailhost.<company.com>
   ```

2. Normalize hostname aliases (CNAME):

   ```
   <uid>@<mail_host_alias>.<company.com> -->
   uid@<mailhost>.<company.com>
   ```

Canonicalizing addresses of this type can be done by including a set of rewrite rules for each non-fully qualified address. The default SIMS configuration includes some of those rules:

CODE EXAMPLE 5-2 SIMS Default Rewrite Rules to Canonicalize Local Addresses

```
! rules to select local users
mailhost.corp.company.com $U%mailhost.corp.company.com      [1]
mailhost.corp $U%mailhost.corp.company.com                  [2]
mailhost $U%mailhost.corp.company.com                       [3]
corp.company.com  $E$U%$D                                   [4]
! tcp_intranet
.corp.company.com  $E$U%$H.corp.company.com                 [5]
*  $U%$&0.corp.company.com@tcp_intranet-daemon              [6]
.corp $U%$H.corp.company.com                                [7]
```

[1] Rule for already fully qualified addresses.

[2] Rewrites: `user@mailhost.corp --> user@mailhost.corp.company.com`

[3] Rewrites: `user@mailhost --> user@mailhost.corp.company.com`

[4] Rule for already fully qualified addresses

[5] Rule for already fully qualified addresses

[6] Rewrites: `user@myhost --> user@myhost.corp.company.com`

[7] Rewrites: `user@myhost.sub.corp ->user@myhost.sub.corp.company.com`

For complex multinational environments which include multiple servers, these rules may be very numerous or subtle. For example:

If our domain is bridge.com, an internal address might be:

```
bill@hourglass.uk     --> bill@hourglass.uk.bridge.com
```

And an external address could be:

```
paul@stream.co.uk --> paul@stream.co.uk
```

In this first example the internal address ends with `.uk` and is canonicalized as needed for internal delivery. In the second example, however, the address ends with `.uk`, but is not an internal address, consequently it shouldn't be canonicalized. Problems like this cannot be solved by adding just one simple re-write rule. That's where DNS-based canonicalization can be useful.

By using the DNS-based canonicalization the administrator can concentrate all the information in one place instead of spreading it across different rewrite rules living in different `imta.cnf` files. Moreover, this information is already available in the DNS database. The disadvantage of DNS-based canonicalization is that for every address (canonicalization is applied to both envelope and header addresses), at least one DNS lookup is issued, making this process much slower than a simple rewrite rule.

DNS-based Canonicalization Algorithm

A SIMS DNS-based canonicalization consists of successive DNS lookups:

1. If the address contains at least one dot, a DNS lookup is attempted on the address as it is.
2. If no record is found with this address, then successive lookups with variations of the domain part of the address are attempted. Those variations are taken from the `domain` or `search` attribute in the `/etc/resolv.conf` file.

   Example 1: If the incoming address domain is `hourglass` with a `search` attribute in `/etc/resolv.conf`) set as follows:

   ```
   search corp.bridge.com bridge.com
   ```

   the successive DNS queries will be `hourglass.corp.bridge.com.` and `hourglass.bridge.com`.

   Example 2: If the incoming address is `hourglass.corp`, the successive DNS queries will be `hourglass.corp.`, `hourglass.corp.corp.bridge.com.` and `hourglass.corp.bridge.com`.

For each DNS lookup:

- If a CNAME record is found for the address, the address is replaced by the new one and the entire process starts again (step 1).
- If an A record is found, the address that was just used to query is considered the canonical address and the address is rewritten.
- If an MX record is found then:
  - If no domain variation was added yet (example: the incoming address was `hourglass.corp.bridge.com`), the hostname that was just used to query is considered the canonical address and the address is rewritten.
  - If no previous MX record were found by previous queries, the hostname is kept but the lookups continue.
  - If a previous MX record was found, that previous record is considered the canonical address and the address is rewritten.

Thus, if the incoming address is `hourglass`, an A record and an MX record are found for the address `hourglass.corp.bridge.com`, then the canonicalized address is `hourglass.bridge.com`.

If the incoming address is hourglass, the first query will try hourglass.corp.bridge.com. If only an MX record is found for this entry, the query is continued for hourglass.bridge.com. If another MX record is found, then hourglass.corp.bridge.com is the canonical address.

Literal to Domain Canonicalization

It is legal to put an IP address in the domain part of an email address if the IP address must be between square brackets “[ ]” (example: rocketeer@[191.24.12.13]). This is known as *literal addressing*. Literal to domain canonicalization replaces this type of address with the canonical one if the reverse DNS lookup for IP address to hostname succeeds. Example:

bob@[192.24.12.12] --> bob@rocket.stream.com where 192.24.12.12 is the IP address of rocket.stream.com.

Setting Up DNS-based Canonicalization

DNS-based canonicalization can’t be set up through the Admin Console. You have to manually include a set of rewrite rules.

The rewrite rules for DNS-based canonicalization are in the file /etc/opt/SUNWmail/imta/dns_canonical.rules. The rule corresponding to the DNS canonicalization is:

```
$* $[IMTA_DNSRULES,imdns_canon_or_tmpfail,$U@$H]
```

The rule corresponding to the literal to domain canonicalization is

```
[] $U%$[IMTA_DNSRULES,imdns_canon_literal,$L]
```

To activate DNS canonicalization, edit /etc/opt/SUNWmail/imta/imta.cnf and uncomment the include line for dns_canonical.rules by removing the leading “!” character):

```
! DNS canonicalization rules
</etc/opt/SUNWmail/imta/dns_canonical.rules
```

Then restart the MTA:

```
/opt/SUNWmail/sbin/imta restart
```

You can activate only the DNS canonicalization or the literal-to-domain functionality by commenting one of them in /etc/opt/SUNWmail/imta/dns_canonical.rules.

Note – These operations will only work if your DNS is accurately configured.

CHAPTER 6

IMTA Security and Unsolicited Bulk Email (UBE) Handling

SMTP Access and Relay Restrictions

The Message Access and Relay Restriction feature allows you to restrict messages from passing through SIMS based on source/destination email address, IP address, and domain. This feature provides several types of functionality:

- Limits unsolicited bulk email (UBE) or spam by blocking unwanted mail
- Limits UBE by not relaying (sending mail from one domain to another) unwanted mail
- Restricts email usage to internal users

SMTP access and relay restrictions rules are located in the mapping file at /etc/opt/SUNWmail/imta/mappings. The mappings file can contain three tables from which to control SMTP access and relay:

- PORT_ACCESS mapping table can be used to control the IP addresses from which IMTA servers will accept connection attempts; the server checks this table when a connection attempt comes in.
- ORIG_SEND_ACCESS mapping table can be used to control access based on the From address, To address, and the source and destination channels.
- ORIG_MAIL_ACCESS mapping table can be used to control email access based on both IP addresses, and From address and To addresses. It essentially combines the functionality of PORT_ACCESS and ORIG_SEND_ACCESS.

SIMS provides a GUI access for adding and modifying rules in these tables (see "Access and Relay Restrictions with the Admin Console" on page 131). However, to implement more complex access controls you'll have to edit the mappings file directly. Refer to the section on the IMTA mapping file in the *SIMS Reference Manual*.

SMTP Access Restrictions by IP Address and Port Number

The SMTP server is able to selectively accept or reject incoming SMTP connections based on IP address and port number. The PORT_ACCESS table is used by the IMTA to selectively accept or reject incoming SMTP connections based on IP address and port number. If the PORT_ACCESS mapping table was present when the IMTA started up, the IMTA checks all connections by formatting the connection information in the form:

```
TCP|server-address|server-port|client-address|client-port
```

The server looks for a match in the PORT_ACCESS table. If the result of the mapping contains $N, the connection is immediately closed. Any other result allows the connection to be accepted. The metacharacter $N may be followed by a rejection message. If present, the message is sent back down the connection just prior to closure. Note that a CRLF terminator is appended to the string before it is sent back down the connection. See TABLE 6-1 on page 126 for additional access mapping flags.

For example, the following mapping will only accept SMTP connections from a single network, except for a particular host singled out for rejection without any message:

```
PORT_ACCESS

  TCP|*|*|192.12310.70|*    $N
  TCP|*|*|192.123.10.*|*     $Y
  TCP|*|*|*|*                $N500$ Bzzzzzzzzt$ thank$ you$ for$ playing.
```

Note that if you are using the PORT_ACCESS mapping table you will need to restart the dispatcher after making any changes to this mapping table so that the IMTA will see the new compiled configuration.

The PORT_ACCESS mapping table is specifically intended for performing only IP number-based rejections; for more general control at the email address level or a combination of email address and port access, the ORIG_SEND_ACCESS mapping table or the ORIG_MAIL_ACCESS table can be used.

Note that you must restart the IMTA after changing the PORT_ACCESS mapping.

SMTP Access Restrictions by Source and Destination Email Address

The ORIG_SEND_ACCESS mapping table may be used to control who may or may not send mail, receive mail, or both. The nature of the mapping is very general and allows per-channel granularity.

If the ORIG_SEND_ACCESS mapping table exists, then for each recipient of every message passing through the IMTA, the IMTA will probe the table with a probe string of the form:

```
src-channel|from-address|dst-channel|to-address
```

The *src-channel* is the channel originating the message (that is, queueing the message); *from-address* is the address of the message's originator; *dst-channel* is the channel to which the message will be queued; and *to-address* is the address to which the message is addressed. Use of an asterisk in any of these four fields causes that field to match any channel or address, as appropriate.

If the probe string matches a pattern that is, the left side of an entry in the table, then the resulting output of the mapping is checked. If the output contains the metacharacters $Y then the enqueue for that particular To address is permitted. If the mapping output contains the metacharacters `$N` then the enqueue to that particular address is rejected. In the case of a rejection, an optional rejection message may be supplied in the mapping output. This string will be returned as a rejection message. If no string is output (other than the `$N` metacharacter), then a default message will be used. See TABLE 6-1 on page 126 for additional access mapping flags.

Suppose that local users in the domain `acme.com`, with the exception of the postmaster, can receive but not send mail to the Internet. Then the `ORIG_SEND_ACCESS` mapping table shown in CODE EXAMPLE 6-1 is one possible way to enforce this restriction. In that example, the local host name is assumed to be `acme.com`. In the channel name `tcp_*`, wildcards are used so as to match any possible TCP/IP channel name. In the rejection message, dollar signs are used to quote spaces in the message. Without those dollar signs, the rejection would be ended prematurely and only read “Internet” instead of “Internet postings are not permitted.”

CODE EXAMPLE 6-1 Restricting Internet Mail Access on UNIX

```
ORIG_SEND_ACCESS

  *|postmaster@acme.com|*|*  $Y
  *|*|*|postmaster@acme.com  $Y
  l|*@acme.com|tcp_*|*      $NInternet$ postings$ are$ not$
permitted
```

TABLE 6-1 Access Mapping Flags (More in the *SIMS Reference Manual*)

Flag	**Description**
$B	Redirect the message to the bitbucket (discard message).[1]
$F	Reject access
$H	Hold the message as a .HELD file
$Y	Allow access
Flags with arguments, in argument reading order+	
$<string	Send string to syslog (UNIX) if probe matches++
$>string	Send string to syslog (UNIX) if access is rejected ++
$Ddelay	Delay response for an interval of delay hundredths of seconds; a positive value causes the delay to be imposed on each command in the transaction; a negative value causes the delay to be imposed only on the address handover (SMTP RCPT TO: command)
$Ttag	Prefix with tag `tag`[1]

TABLE 6-1 Access Mapping Flags (More in the *SIMS Reference Manual*) *(Continued)*

Flag	Description
$Aheader	Add the header line header to the message[1]
$Xerror-code	Issue the specified extended SMTP error code if rejecting the message[1]
$Nstring	Reject access with the optional error text string

[1] Not applicable for SMTP access restrictions by IP address and port number because these restrictions are applied before the SMTP dialog starts

SMTP Access Restrictions by IP Address, Port, and Email Address

The ORIG_MAIL_ACCESS mapping table combines the two previous mapping tables: ORIG_SEND_ACCESS and PORT_ACCESS. The syntax is similar (it should appear on one line):

TCP|*server-address*|*server-port*|*client-address*|*client-port*|SMTP|MAIL|*src-channel*|
from-address|*dest-channel*|*to-address*

For example, to allow abc.com to relay mail through your domain only if the mail is submitted from the IP address 192.9.9.9, use the following mapping:

```
ORIG_MAIL_ACCESS

  TCP|*|*|192.9.9.9|*|SMTP|MAIL|tcp_local|*@abc.com|tcp_local|*    $Y
  TCP|*|*|*|*|SMTP|MAIL|tcp_local|*@abc.com|tcp_local|*            $N
```

ORIG_SEND_ACCESS is looked up first. If ORIG_SEND_ACCESS has a rule which supersedes the rule in ORIG_MAIL_ACCESS, the rules in ORIG_MAIL_ACCESS will not be used at all. See TABLE 6-1 on page 126 for additional access mapping flags.

Limiting the Number of Recipients Per Message or the Number of Messages Per Session

You can use two SMTP channel options ALLOW_TRANSACTIONS_PER_SESSION and ALLOW_RECIPIENTS_PER_TRANSACTION to implement dynamic rejection mechanisms. The ALLOW_TRANSACTIONS_PER_SESSION option can be used to limit the number of messages accepted during a particular connection. After refusing a number of connection attempts from a particular site, once you do let them connect, they are liable to have a backlog of messages for your site which they will try to deliver during that connection. If you are attempting to “slow down” how much mail you accept from that site, you likely will want to use this option to say, in effect, “enough for now” after some point in the connection. Similarly, the ALLOW_RECIPIENTS_PER_TRANSACTION option can be used to limit the number of recipients allowed for a particular message; this can be useful in protecting against a denial of service attack in the form of messages blanketing large numbers of your users.

These options can be access through the Admin Console. See “To Configure Message Limitation” on page 101 and “To Set Recipient Limitation” on page 106

DNS-based Email Access Control

Spammers often disguise their email address by using a fake From: address with a fake domain name. You can set up your server to only accept mail from addresses that have valid domains in the DNS. dns_verify is a program that allows you to do this. dns_verify can be turned on or off using the mailfromdnsverify keyword (see the *SIMS Reference Manual*). Note that configuring manually in the mapping files gives more control on error messages.

Given a domain, the dns_verify program queries the DNS to check if either an A record or an MX record exists for the domain. If either record exists, dns_verify accepts, otherwise, it rejects.

Setting up dns_verify

The dns_verify program is used in a mapping rule in the mappings file (see section on the Mapping File in the *SIMS Reference Manual*). The rule can come under either the ORIG_SEND_ACCESS and ORIG_MAIL_ACCESS tables.

Examples for each usage are shown below. Each entry must appear on a single line, even though they are shown here on multiple lines for readability.

```
ORIG_SEND_ACCESS
*|*@*|*|*  $[/opt/SUNWmail/imta/lib/dns_verify,dns_verify,
     $2|$$Y|$$NInvalid$ host:$ $$2$ -$ %e]
```

```
ORIG_MAIL_ACCESS
TCP|*|*|*|*|SMTP|MAIL|*|*@*|*|*  $[/opt/SUNWmail/imta/lib/dns_verify,
     dns_verify,$6|$$Y|$$NInvalid$ host:$ $$6$ -$ %e]
```

/opt/SUNWmail/imta/lib/dns_verify is the library and dns_verify is the function. The complete syntax for these entries is described in “SMTP Access Restrictions by Source and Destination Email Address” on page 125 and the section on the Mapping File in the *SIMS Reference Manual*.

dns_verify Arguments

The argument to dns_verify has three parts delimited by '|' as shown below:

```
hostname|return-if-good|return-if-bad
```

The return-if-good and return-if-bad strings are templates for the return string. If hostname has a valid DNS entry, the return-if-good template is used to generate a return string. Otherwise, the return-if-bad template is used.

These are the format characters you can include in the return-if-good and return-if-bad strings:

%a - If successful, the IP address found from the DNS lookup

%n - If successful, the primary name for this host

%e - The error message associated with the lookup

Continuing from the first example above:

```
  $2|$$Y|$$NInvalid$ host:$ $$2$ -$ %e
```

With this argument string, “$Y” is returned when $2 has a valid DNS entry. If $2 does not have a valid DNS entry, the return string would look something like this:

```
$NInvalid host: eng.sun.com - authoritative host not found: usr001
                ~~~~~~~~~~    ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
                    $2                     %e
```

Notice how dollar signs and spaces need to be quoted. They appear as "$$" and "$ " respectively.

Using dns_verify to Lookup Realtime Spam Sites

It is possible to use `dns_verify` to look up addresses on a realtime black hole list by setting `ENABLE=1` in your Dispatcher configuration file (`/etc/opt/SUNWmail/imta/dispatcher.cnf`) and by creating the appropriate `dns_verify` entry in your `PORT_ACCESS` mapping table in the `mappings` file. Below is an example:

```
PORT_ACCESS
TCP|*|25|*.*.*.*|*       $[/opt/SUNWmail/imta/lib/
dns_verify,dns_verify,\
+$4.$3.$2.$1.rbl.maps.vix.com\
+$$N500$ 5.7.1$ Mail$ from$ $$1.$$2.$$3.$$4\
$ refused,$ see$ http://maps.vix.com/rbl/\
+$$CTCP|$$0|25|$$1.$$2.$$3.$$4|$$5\
+$$CTCP|$$0|25|$$1.$$2.$$3.$$4|$$5]
```

This `dns_verify` string checks the DNS for an A record for `D.C.B.A.rbl.maps.vix.com`. If it finds such a record (indicating that the system with address `A.B.C.D` is on the RBL), it returns the error "500 5.7.1 Mail from A.B.C.D refused, see http://maps.vix.com/rbl/". If it sees that the DNS query returns that the record didn't exist, or it was unable to determine (DNS "Server failed" error), it will continue the mapping probe looking for other possible matches. If no match is found, the connection is permitted. For detailed information about the syntax, refer to the *SIMS Reference Manual*.

If you have any other `PORT_ACCESS` entries, put them after this one. If this one does not find that a particular incoming IP address is on the list, it will continue the probe in the mapping table.

Limitations

Rejecting mail based on the absence of a DNS record is not supported by Internet RFCs. RFC822 and RFC1123 direct that mail addressed to postmaster must not be rejected. Violation of this is sufficient cause for your domain to be disconnected from the Internet.

Also, if your DNS is unstable or experiences an outage, mail you might otherwise accept will be rejected.

It is strongly recommended that you have a rule accepting all mail to the postmaster before the `dns_verify` rule is applied. Example,

```
ORIG_SEND_ACCESS
```

```
   *|*@*|*|postmaster@localhost.domain    $Y
   *|*@*|*|*  $[/opt/SUNWmail/imta/lib/dns_verify,dns_verify,
                $2|$$Y|$$NInvalid$ host:$ $$2$ -$ %e]
```

Known Limitations

On systems where `nsswitch.conf` is configured such that some other source comes after DNS in the hosts database, for example:

```
hosts:     dns nis files
```

senders with mail domains without `A` records in DNS will be rejected even if they do have `MX` records. This bug is due to `gethostbyname()` not returning the appropriate error code which `dns_verify` depends on.

This bug will not manifest itself on systems configured with DNS as the last source for the hosts database or with `[NOTFOUND=return]` for DNS. For example,

```
hosts:     dns
hosts:     dns [NOTFOUND=return] nis
```

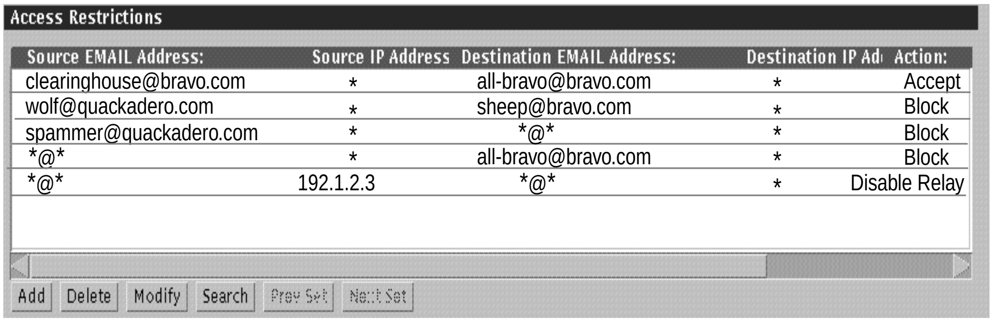
Also, `dns_verify` is not supported by SIMS Admin Console. Changes to the mappings file have to be done by hand using a text editor. The Admin Console will overwrite the `dns_verify` entries the next time it modifies the mappings file.

Access and Relay Restrictions with the Admin Console

AdminConsole>IMTA>Access Restrictions

1. **In the Sections list of the IMTA property book, click Access Restrictions.**

   The Access Restrictions section appears.



Access Restrictions

Source EMAIL Address:	Source IP Address	Destination EMAIL Address:	Destination IP Ad	Action:
clearinghouse@bravo.com	*	all-bravo@bravo.com	*	Accept
wolf@quackadero.com	*	sheep@bravo.com	*	Block
spammer@quackadero.com	*	*@*	*	Block
@	*	all-bravo@bravo.com	*	Block
@	192.1.2.3	*@*	*	Disable Relay

FIGURE 6-1 Access Restrictions Section

A list of the first 50 *access restriction rules* appears in the display (press Next Set or Prev Set to display the next or previous 50 rules). An access restriction rule is a rule applied to a message, which determines whether SIMS will block or accept the message. The order of rules displayed is the order in which each rule is applied to an incoming message before forwarding the message. The first rule that applies to the message will have its action applied to the message. Each rule consists of the following parameters:

Source EMAIL Address is the address of the sender on which to take action.

Source IP Address is the client IP address from which a message has been sent.

Destination EMAIL Address is the address of the recipient of the mail.

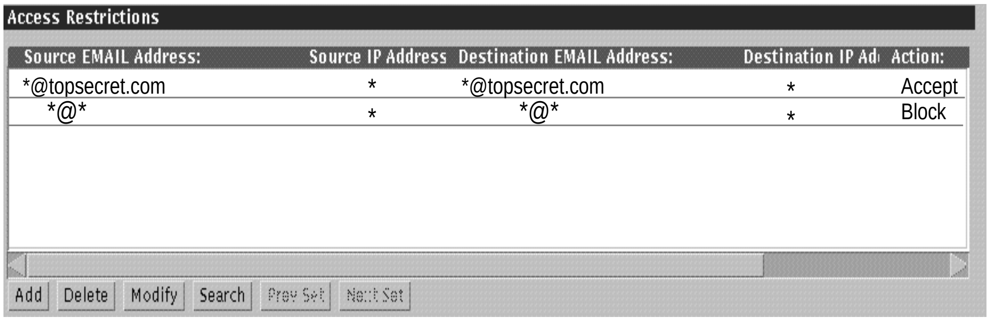
Destination IP Address is the server IP address at which the mail has been received.

Action is the action to take for a message specified by the preceding parameters. It can be *Accept* (accept message or forward to next stop), *Block* (refuse message delivery and return to sender), *Disable Relay* (refuse message from an external domain directed to another external domain and return mail to sender with the message "`Relaying not permitted`"). Rules based on IP addresses alone are applied before all other rules. If the `/etc/opt/SUNWmail/imta/mappings` file is edited by hand to include any other action, it will be shown as an asterisk (*) in the console.

Rules are automatically sorted from most to least specific with *Source EMAIL Address* being used as the primary sort key, and *Destination EMAIL Address* being used as the secondary key. For example, a rule with a source email address as `*@stork.env.sunny.com` would be higher on the list compared to a rule with source email address `*@*.env.sunny.com`.

In FIGURE 6-1 the first rule allows `clearinghouse@bravo.com` to send messages to `all-bravo@bravo.com`. The second rule blocks mail from `wolf@quackadero.com` to `sheep@bravo.com`. The third rule blocks mail from spammer@quackadero.com from being delivered. The fourth rule blocks delivery of mail to all-bravo@bravo.com. The fifth rule stops inter-domain messages from IP address 192.1.2.3 from being delivered to the next domain.

You could also configure users within a particular company or group to be restricted to only sending mail to each other. The access rules for this are shown below.

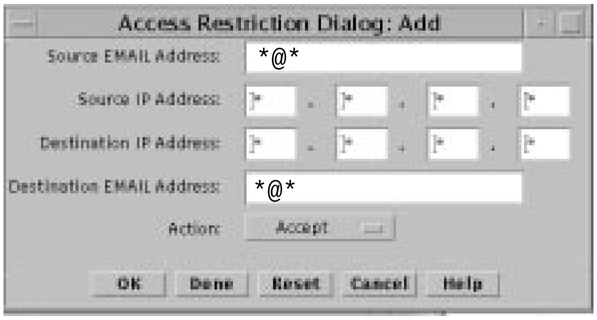


Access Restrictions

Source EMAIL Address:	Source IP Address	Destination EMAIL Address:	Destination IP Ad	Action:
*@topsecret.com	*	*@topsecret.com	*	Accept
@	*	*@*	*	Block

FIGURE 6-2 Restricting Access to Users within a Company

2. **To add an Access Restriction rule, click Add. The Access Restriction Dialog appears:**



Access Restriction Dialog: Add

Source EMAIL Address: *@*

Source IP Address: * . * . * . *

Destination IP Address: * . * . * . *

Destination EMAIL Address: *@*

Action: Accept

FIGURE 6-3 Access Restriction Dialog

a. **Specify the desired Access Restriction parameters and click Done.**

Enter email addresses for the Source and Destination EMAIL Address fields. Asterisks may be used as a wild card character. If no IP address is entered, the default *.*.*.* is entered.

Asterisks will be allowed on source or destination addresses. Otherwise, addresses must contain a local part and a domain part, separated by an @ sign. The wild-card character (*) can be used, with the following restrictions:

i. **Wild cards in addresses cannot be used on the right of non-wild-carded areas. That is: `username@*, username*@*`, or `username@japan.*` are illegal, `*@*.com`, `*@xyz.com` are legal.**

ii. **Wild cards cannot be used within an address token. A wild card may only replace one or more entire domain part token. For instance, `*@*sun.com` is illegal.**

iii. **Wild cards may be used in local parts as long as they replace the entire user name. As such, `username*@sun.com` is illegal.**

b. **Resolve conflicting rules.**

If you try creating a rule that conflicts with previously written rule, the Admin Console will bring up a dialog box that shows all the rules with which the current rule conflicts. You must then resolve the conflict by modifying the fields of the rule.

An example of a conflicting rule is shown below:

	Rule A	**Rule B**
Source address:	`*@*.quacky.com`	`*@*.quacky.com`
Destination address:	`*@eng.bravo.com`	`*@eng.bravo.com`
Action:	`Block`	`Accept`

A conflict occurs if a message from `usr1@eng.quacky.com` is addressed to `usr2@eng.bravo.com`. Rule A says to block this message, and rule B says to accept. This conflict must be resolved before the new rules will be accepted. (More complex rules conflicts might occur; see “Conflicting Access Restriction Rules” on page 135 for a more in-depth discussion.)

c. **After a rule is set, press OK to add the rule and keep dialog up, or press Done to add the rule and close the dialog.**

To save the rules, press Apply. You are prompted to restart the IMTA, which will incorporate the new or modified rule.

3. **To modify an Access Restriction rule, select the rule and click Modify.**

   Modify parameters as you prefer and press Apply to save.

4. **To delete an Access Restriction rule, select the rule and click Delete and Apply.**

5. **To search for an Access Restriction rule, click Search and add the search parameters in the Access Restriction Dialog.**

   You can use the wild card (*) character. Search is used for finding a particular set of access restriction rules that you wish to modify, verify, or delete.

Conflicting Access Restriction Rules

The previous section described a very obvious case of rules conflict. A less obvious case of conflict arises when Rule 1 is less specific than Rule 2 according to one parameter, and more specific than Rule 2 according to another parameter. For example, suppose we have defined the following two rules:

	Source address:	**Destination address:**	**Action:**
Rule 1	`*@hosta.a.com`	`*@*.b.com`	`Block`
Rule 2	`*@*.a.com`	`*@hostb.b.com`	`Accept`

These rules would not resolve the scenario where mail from `*@hosta.a.com` is to be delivered to `*@hostb.b.com`. To create a set of rules that would address the various delivery scenarios involved with these two addresses, we need to determine whether to block or deliver in these two specific scenarios:

	Source address:	**Destination address:**	**Action:**
Scenario 1	`*@hosta.a.com`	`*@hostb.b.com`	?
Scenario 2	`*@*.a.com`	`*@*.b.com`	?

The outcomes of these scenarios would be described by Rules 3 and 4 described below in the Outcome sections. These rules might or might not already exist.

The following matrix shows Scenarios 1 and 2, their specified actions (Block or Accept), and the rules needed to create the desired outcomes.

Scenario 1 **Scenario 2**	Block	Accept
Block	Outcome A: Scenario 1-Block Scenario 2-Block	Outcome B Scenario 1 - Accept Scenario 2 - Block
Accept	Outcome C Scenario 1-Block Scenario 2-Accept	Outcome D Scenario 1 - Accept Scenario 2 - Accept

Outcome A

Here are rules resolving Outcome A. (Rule 1 is not necessary, it is displayed for edification.) Rules are displayed in the sorted order: from most to least specific, with *Source* being the primary key; *Destination* being the secondary key; and the order in which each rule would be applied to an incoming message before forwarding.

	Source address:	**Destination address:**	**Action:**
Rule 3	`*@hosta.a.com`	`*@hostb.b.com`	`Block`
*** Rule 1**	`*@hosta.a.com`	`*@*.b.com`	`Block`
Rule 2	`*@*.a.com`	`*@hostb.b.com`	`Accept`
Rule 4	`*@*.a.com`	`*@*.b.com`	`Block`

- Rule 1 is not needed because in the following delivery scenario the delivery is not matched by Rule 2 and covered by Rule 4:

  ```
  *@hosta.a.com  ——>  *@<any host but hostb>.b.com
  ```

- Rule 3 is needed because Rule 2 applies to the following scenario. The conflict can be resolved by using the rules 2, 3, and 4. Rule 4 might not be needed if it is covered by a more generic rule.

  ```
  *@hosta.a.com  ——>  *@hostb.b.com
  ```

Outcome B

Here are the rules needed to resolve Outcome B:

	Source address:	**Destination address:**	**Action:**
***Rule 3**	`*@hosta.a.com`	`*@hostb.b.com`	`Accept`
***Rule 1**	`*@hosta.a.com`	`*@*.b.com`	`Block`
Rule 2	`*@*.a.com`	`*@hostb.b.com`	`Accept`
Rule 4	`*@*.a.com`	`*@*.b.com`	`Block`

- Rule 1 is not needed because in the following delivery scenario

  ```
  *@hosta.a.com  ——>  *@<any host but hostb>.b.com
  ```

  the delivery is not matched by Rule 2 and covered by Rule 4.
- Rule 3 is not needed because Rule 2 applies to the scenario

  ```
  *@hosta.a.com  ——>  *@hostb.b.com
  ```

Hence the conflict can be resolved by using Rules 2, and 4. Rule 4 might not be needed if it is covered by a more generic rule.

Outcome C

Here are the rules needed to resolve Outcome C:

	Source address:	Destination address:	Action:
***Rule 3**	`*@hosta.a.com`	`*@hostb.b.com`	`Block`
Rule 1	`*@hosta.a.com`	`*@*.b.com`	`Block`
***Rule 2**	`*@*.a.com`	`*@hostb.b.com`	`Accept`
Rule 4	`*@*.a.com`	`*@*.b.com`	`Accept`

- Rule 2 is not needed because in the following delivery scenario

  ```
  *@<any host but hosta>.a.com  ——>  *@hostb.b.com
  ```

  the delivery is covered by Rule 4 and doesn't match Rule 1.
- Rule 3 is not needed because Rule 1 applies to the scenario

  ```
  *@hosta.a.com  ——>  *@hostb.b.com
  ```

Hence the conflict can be resolved by using Rules 1 and 4. Rule 4 might not be needed if it is covered by a more generic rule.

Outcome D

Here are the rules needed to resolve Outcome D:

	Source address:	Destination address:	Action:
***Rule 3**	`*@hosta.a.com`	`*@hostb.b.com`	`Accept`
Rule 1	`*@hosta.a.com`	`*@*.b.com`	`Block`
***Rule 2**	`*@*.a.com`	`*@hostb.b.com`	`Accept`
Rule 4	`*@*.a.com`	`*@*.b.com`	`Accept`

- Rule 2 is not needed because in the following delivery scenario

  ```
  *@<any host but hosta>.a.com  ——>  *@hostb.b.com
  ```

  the delivery is not matched by Rule 1 and is covered by Rule 4.
- Rule 3 is needed because Rule 1 applies to the scenario

  ```
  *@hosta.a.com  ——>  *@hostb.b.com
  ```

Hence the conflict can be resolved by using Rules 1, 3, and 4. Rule 4 might not be needed if it is covered by a more generic rule.

Note – There is no warning mechanism for rules added by manually editing the IMTA Mappings File. You must be very careful about creating conflicting rules.

Optimizing Access and Relay Restrictions

Utilities: `libimtamap`

The SIMS IMTA access and relay restriction feature can cause a reduction in IMTA performance if there are too many anti-spam rules. SIMS provides a set of mapping loadable routines that can be used to increase the efficiency of anti-spamming configurations in the IMTA. Note that these routines can only be used by editing the mapping file. Refer to the section on the IMTA mapping file and the chapter on IMTA Security in the *SIMS Reference Manual*.

Note – If you use any of these mapping loadable programs, the Access Restriction section of the Admin Console will not be visible, and you will have to view the rules by looking at the mappings file.

Rules Optimization

In most cases, anti-spamming rules are directed toward a specific goal such as allowing relay for a specified client IP address or blocking mail whose envelope contains a specified string. For these types of rules, the decision is based on a single parameter. For example:

```
ORIG_SEND_ACCESS
*|spammer1|*|* $NNone$ of$ this$ here
*|spammer2|*|* $NNone$ of$ this$ here
*|spammer3|*|* $NNone$ of$ this$ here
*|spammer4|*|* $NNone$ of$ this$ here
*|spammer5|*|* $NNone$ of$ this$ here
```

Due to the way mapping tables work, the mapping process goes through all rules sequentially until a definite match is found. If you have more than 30 rules in which a single parameter defines the decision, then you may find that using the process described below will optimize the servers ability to handle multiple rules.

SIMS provides routines that increase the SMTP server performance when a large number of similar mapping rules are used. These routines can be used to replace multiple rules which have a common single parameter that varies in the pattern.

To use these routines, the list of values of this varying parameter are stored in a plain text file called a *resource file*, one parameter value per line. Several rules can be used to reference different resource files. Each of these resource files is loaded only once per process, the first time it's used.

The format of a rule is as follows:

```
*|*|*|* $[/opt/SUNWmail/imta/lib/libimtamap.so,
<routine>,$1|<resource file>|<string>]
```

`*|*|*|*` is the format of a `send_access`/`port_access` rule.

`libimtamap.so` is the library.

`<routine>` is either `immap_is_in_list`, `immap_is_in_cilist`, or `immap_is_in_list_of_ip`.

`$1` refers to the second * in the first argument, which is the source email address in `send_access` table or server IP address in the `port_access` table.

`<resource file>` is the path of the resource file.

`<string>` the string to put in result if a match is found.

The routines look up the parameter in a hash table created from the resource file and returns successfully if it is found. If successful, the routine can either set the result string according to the argument or to a hard-coded values. Upon failure, the mapping process continues with the next rule.

`immap_is_in_list` returns successfully if the string parameter is in the resource file. `immap_is_in_list` is the case-insensitive version of the same function. `immap_is_in_list_of_ip` returns successfully if the IP address parameter is within one of the networks contained in the resource file.

▼ To Optimize Access and Relay Restrictions Performance

1. **Determine if you have multiple rules with a single changing parameter in each rule.**

2. **List of values of the varying parameter in a plain text file.**

   Use one value per line, several rules can be used to reference different resource files. For example, if this is the original table:

   ```
   ORIG_SEND_ACCESS
   *|spammer1|*|* $NNone$ of$ this$ here
   *|spammer2|*|* $NNone$ of$ this$ here
   ```

```
*|spammer3|*|* $NNone$ of$ this$ here
*|spammer4|*|* $NNone$ of$ this$ here
*|spammer5|*|* $NNone$ of$ this$ here
```

Then the resource file, which for this example we call `/tmp/bad_from.txt`, would be:

```
spammer1
spammer2
spammer3
spammer4
spammer5
```

3. **Replace the original rules with a single new rule using `immap_is_in_list` or `immap_is_in_list_of_ip`**

```
ORIG_SEND_ACCESS
*|*|*|* $[/opt/SUNWmail/imta/lib/libimtamap.so,
immap_is_in_list,$1|/tmp/bad_from.txt|$$NNo$ Spam$ Allowed$
Here]
```

Any mail from someone in the `bad_from.txt` file will be returned to the sender with the message `No Spam Allowed Here`. The case-independent version is called `immap_is_in_cilist`. It is particularly useful when dealing with domains which are case-insensitive.If you are blocking IP addresses, use the command `immap_is_in_list_of_ip`.

SMTP AUTH Configuration

SMTP AUTH is by default turned off. It can be activated by using the `maysaslserver`, `mustsaslserver`, `nosaslserver`, `nosasl`, and `saslswitchchannel` channel keywords in the appropriate SMTP channel blocks (`imta.cnf`). The channels keywords are described in more detail in the *SIMS Reference Manual*. Refer to the *SIMS Concepts Guide* for conceptual information.

`nosasl` is the default, and means that SASL authentication will not be permitted or attempted. It subsumes `nosaslserver`.

`nosaslserver` specifies that SASL authentication will not be permitted.

`maysaslserver` causes the SMTP server to permit clients to attempt to use SASL authentication.

`mustsaslserver` specifies that the SMTP server insist that clients use SASL authentication; the SMTP server will not accept messages unless the remote client successfully authenticates.

saslswitchchannel is used to cause incoming connections to be switched to a specified source channel upon a client's successful SASL use. It takes a required value, specifying the channel to which to switch.

SMTP AUTH Example 1

A site that generally blocks SMTP relaying through their SMTP server, but wishes to allow such SMTP relaying for specific users who will authenticate themselves using SASL, might use channel definitions similar to these given below. This type of configuration is particularly appropriate for sites wanting to allow roaming users to keep relaying mail through their domain's mail server, while preventing other users to do the same.

In imta.cnf:

```
tcp_local smtp mx single_sys maysaslserver saslswitchchannel tcp_auth
tcp-daemon

tcp_auth smtp mx single_sys mustsaslserver
tcp-auth-daemon
```

with an ORIG_SEND_ACCESS mapping table (/etc/opt/SUNWmail/imta/mappings) like this:

```
ORIG_SEND_ACCESS

tcp_local|*|tcp_local|*     $NRelaying$ not$ permitted
```

An attempt to submit a message with no authentication would go straight back out the tcp_local channel and therefore would be rejected due to the ORIG_SEND_ACCESS entry shown.

But if a connection from an external system performs SASL authentication, the connection is switched to the tcp_auth channel. The tcp_auth channel will not allow messages submission unless the remote connecting client successfully authenticates itself. For connections that do authenticate, the messages will be accepted on the tcp_auth channel, and may be relayed out through the tcp_local channel, should that be the appropriate destination channel.

SMTP AUTH Example 2

A similar example would be for a site that also allows relaying by internal clients or systems as well as authenticated external clients. Such a configuration will use the switchchannel keyword and rewrite rules to identify and switch “internal” connections to the tcp_intranet channel:

imta.cnf (rules)

```
.bridge.net     $U%$H$D@tcp_intranet-daemon
[1.2.3.]        $E$R$U%[1.2.3.$L]@tcp_intranet-daemon
```

imta.cnf (channel blocks)

```
tcp_local smtp mx single_sys maysaslserver saslswitchchannel
tcp_intranet switchchannel
tcp-daemon

tcp_intranet smtp mx single_sys maysaslserver allowswitchchannel
tcp_intranet-daemon
```

with an ORIG_SEND_ACCESS mapping table like this:

```
ORIG_SEND_ACCESS
tcp_local|*|tcp_local|*     $NRelaying$ not$ permitted
```

Connections from internal systems will be switched to the tcp_intranet channel. That channel will permit SASL use (though clients need not bother to use SASL). Connections from external systems that use SASL to authenticate will be switched to tcp_intranet. Messages from internal users or external users who use SASL authentication will be permitted to be submitted to the Internet. But all other attempted messages submissions from external systems, to attempted Internet destinations, will be rejected due to the ORIG_SEND_ACCESS entry.

Important Warning:

The PLAIN SASL mechanism implies that user passwords are sent in clear text. Passwords should never be sent in clear test in an untrusted environment unless over Transport Layer Security protocol (SSL) or other forms of encrypted TCP/IP connection.

What this means is that SMTP AUTH with the PLAIN mechanism can only be used in a trusted network environment. In the near future, SIMS will support encrypted SMTP connections, which will allow the PLAIN SASL mechanism to be used in untrusted environments as well.

Controlling SMTP Connections and Transactions

- "Identifying the Source of Incoming SMTP Messages" on page 143
- "Logging Messages Passing Through IMTA" on page 143
- "Snapshot of Message Traffic Through IMTA" on page 144

This section points out some message logging and tracking techniques.

Identifying the Source of Incoming SMTP Messages

SIMS provides a variety of channel keywords (for example, `identtcp`, `identtcplimited`) for identifying the sources of incoming SMTP messages. See the Reverse DNS and IDNET Lookups on Incoming SMTP Connections section in the *SIMS Reference Manual* for more details on these channel keywords.

Logging Messages Passing Through IMTA

The `logging` channel keyword causes IMTA write a log file entry for each pass of a message through a IMTA channel. Note that with logging turned on, the cumulative `mail.log` file in the IMTA log directory will continue to grow and grow; IMTA itself never does anything with this log file and it is up to you to periodically write it to backup and delete it, or truncate it, or whatever you prefer.

In addition to the base set of data logged when the `logging` keyword is used, there are options to cause the log output to include additional details, as discussed below.

Extra Logging Detail

In addition to the base set of logging enabled via the logging channel keyword, IMTA has options that cause additional information to be included in the entries written to the mail.log* files. Note that logging such additional information tends to incur additional overhead.

In particular, setting LOG_MESSAGE_ID=1, LOG_CONNECTION=1, and LOG_FILENAME=1 in your IMTA option file may be of interest on a IMTA email firewall. Logging the message ID makes it easier to find entries in the log file corresponding to a particular message, or to correlate different entries in the log file corresponding to a single message. Logging the SMTP client connection information can be useful to show just what system really sent the message to your IMTA firewall. Logging the filename can be useful if you wish to correlate log file entries with actual message files currently in the IMTA queue area.

Setting LOG_HEADER=1 may be of interest if you wish to save certain message headers to the mail.log* files.

Additionally, setting LOG_PROCESS=1 and LOG_USERNAME=1 on a IMTA firewall system ought generally to result in fairly monotonous extra information being logged: the process id of the process enqueuing a message on a IMTA firewall system would normally be that of a IMTA Worker Process (for SMTP messages), and the user name would normally just be the user name of the user who last started the IMTA Service Dispatcher. Enable these options if you wish to confirm that the process ids and usernames of processes enqueuing messages are as expected.

Snapshot of Message Traffic Through IMTA

IMTA maintains channel counters based on the Mail Monitoring MIB, RFC 1566. These counters can provide “snapshots” of the state of the IMTA queues as well as a feel for the volume of messages passing through IMTA.Refer to the *SIMS Reference Manual*.

Controlling Delivery by Email Content and Message Priority

This section discusses imposing limits on the size or sensitivity of messages allowed through, and the related issue of setting message priority based on size, and general checking or filtering of message content.

Imposing Message Size Limits

The IMTA options BLOCK_LIMIT and LINE_LIMIT can be used to impose global size limits on all IMTA channels. The channel keywords blocklimit and linelimit can be used to impose size limits on specific channels. These parameters can also be specified using the Admin Console, see "Message Limitation" on page 101.

Message Priority Limits

IMTA jobs pay attention to message priority, i.e., to the presence of a Priority: header in the message. The priority of message that IMTA immediate jobs (those jobs created when a message is first submitted) will handle may be controlled with the immnonurgent, immnormal, and immurgent channel keywords. The priority of message that IMTA periodic jobs (those jobs run periodically by IMTA to retry delivery of previously undelivered messages) will handle may be controlled with the minperiodicpriority and maxperiodicpriority keywords.

Some sites may wish to control the time of day, for instance, at which low priority messages are sent. And note that the nonurgentblocklimit, normalblocklimit, and urgentblocklimit keywords may be used to forcibly downgrade the priority of "large" messages.

Imposing Message Sensitivity Limits

The channel keywords sensitivitynormal, sensitivitypersonal, sensitivityprivate, and sensitivitycompanyconfidential may be used to impose an upper limit on the sensitivity of messages that may be enqueued to a channel. For instance, a site wishing not to emit messages of Company-confidential sensitivity might choose to set sensitivityprivate on their channel that sends out to the Internet, generally a tcp_local channel.

Checking or Filtering Message Content

The best protection against problematic message content *coming into* your site is educated users who are committed to implementing your site security policies. The best protection against problematic message content *leaving* your site is educated users who are committed to conforming to your site security policies. If the users wish to evade your policies, they can generally work around any imposed restrictions, for instance, by encrypting their messages.

If you do wish to check the actual content of message parts, the IMTA conversion channel can be useful. You may use a `CONVERSION` mapping table to direct that certain message traffic, that is messages coming in certain channels and going out certain channels, pass through the IMTA conversion channel. The IMTA conversion channel can then run whatever content checking or filtering procedure or utility you wish.

For instance, some sites like to have binary message attachments checked by virus sniffing software. A *CONVERSION* mapping table along the lines of

```
CONVERSION
  IN-CHAN=*;OUT-CHAN=tcp_internal;CONVERT      Yes
```

and IMTA conversions file entries along the lines of

```
out-chan=tcp_internal; in-type=application; in-subtype=*;
  command="yourviruscheckcommand ’INPUT_FILE’ ’OUTPUT_FILE’"

out-chan=tcp_internal; in-type=audio; in-subtype=*;
  command="yourviruscheckcommand ’INPUT_FILE’ ’OUTPUT_FILE’"

out-chan=tcp_internal; in-type=image; in-subtype=*;
  command="yourviruscheckcommand ’INPUT_FILE’ ’OUTPUT_FILE’"

out-chan=tcp_internal; in-type=video; in-subtype=*;
  command="yourviruscheckcommand ’INPUT_FILE’ ’OUTPUT_FILE’"
```

where *yourviruscheckcommand* is a site-supplied command to do virus checking, will run any MIME message parts of type APPLICATION, AUDIO, IMAGE, or VIDEO MIME through your procedure.

Note that when you are using the conversion channel to check message parts on the IMTA firewall system, you are likely to want the defragment channel keyword on outgoing channels, particularly channels that send to internal systems. The MIME format allows for messages to be split into multiple pieces, which are normally not reassembled until arrival at the final destination system. However, if you want the intermediate IMTA firewall system to check the message content, you will want to reassemble the message parts on the IMTA firewall system, so that the message content (rather than message content fragments) can be checked.

Firewall Configuration

An email firewall refers to an enhanced, firewall-oriented email handling component on an Internet firewall system. A basic Internet firewall system generally controls what TCP/IP interactions are allowed between the external world, considered to be unsafe, and an internal, protected environment, considered to be safe. To be an email firewall system, this system should also check and control the email passing between the internal and external environments.

- An email firewall system may perform address transformations, converting external presentation addresses in messages incoming from the external world to actual internal addresses, and transforming internal addresses to external presentation addresses on messages outgoing to the external world.
- A firewall system may enforce restrictions on what messages are allowed in or out. In particular, an e-mail firewall may disallow certain sorts of message traffic, and may be configured to protect against denial of service attacks.
- An email firewall is careful in what information it emits in response to external system's possible probe attempts.

Separating External and Internal Message Traffic

One of the fundamental issues for a firewall configuration tends to be separation between internal and external messages. Separating message traffic allows for tracking and appropriately controlling the different sorts of messages. This means separate channels have to be set up to handle messages originating from external sites versus messages originating from internal systems. Internally, the SMTP internet channel is called `tcp_local` while the SMTP intranet channel is called `tcp_intranet`.

A SIMS installation will by default have two SMTP channels, an SMTP intranet and SMTP internet channel, configured for this purpose, if during installation it was specified that this mail server is on a firewall system connected to the internet. This setting can also be done through the Admin GUI's IMTA property book page, after installation. (Refer to "To Configure IMTA Position Relative to the Internet" on page 91).

To achieve the separation of message traffic, rewrite rules are added to associate all internally originating traffic with the `tcp_intranet` channel. The `switchchannel` keyword is added to the `tcp_local` channel. The `noswitchchannel` keyword is added to all other channels except `tcp_intranet`, because by default, the IMTA allows any channel to be “switched to”; i.e, the default is `allowswitchchannel`, and this is not desirable on a firewall system. (Refer to the *SIMS Reference Manual* for information on channel keywords.)

So in order to allow internal systems to be recognized even if a DNS reverse lookup for the incoming IP connection fails, you should use IP literal rewrite rules to associate internal IP literals (at least during backwards envelope rewriting) with your internet SMTP channel. If you wish to limit the rewriting of internal IP addresses to actual system names in the forward direction, say if you do not wish to allow external users to “probe” for internal IP address/internal system name correspondences, then you may want these IP literal rewrite rules to be backwards envelope specific, i.e., `$E$R` rewrite rules.

It is possible to tell the IMTA to not perform DNS reverse lookups, in which case these IP-based rules are mandatory in order to distinguished internal traffic from external traffic. The DNS reverse lookup is turned off by using the `indentnonenumeric` channel keyword.

When a message comes through to the `tcp_local` channel, the IMTA performs a DNS reverse lookup on the incoming IP address. If the reverse lookup succeeds in returning a domain name, IMTA uses that name (and otherwise uses the literal IP address of the incoming connection) to do a reverse-pointing envelope rewrite looking for an associated channel. The rewrite rules associated with the `tcp_intranet` channel helps the IMTA determine whether to “switch” or not.

Note that the default incoming TCP/IP channel is `tcp_local` and only system names recognized as internal system names are “switched” to the `tcp_intranet` channel. This provides “fail-safe” behavior; systems not specifically recognized (even internal systems, if the MTA configuration has not been set up to recognize them) are handled by the external, “unsafe” channel.

Sample configuration of smtp channels on a firewall system

```
!Rewrite rules
..........
! tcp_intranet
.acme.com $E$U%$H.acme.com@tcp_intranet-daemon
* $U%$&0.acme.com@tcp_intranet-daemon
acme $U%acme.com@tcp_intranet-daemon
[a.b.] $R$U%[A.B.$L]@TCP_INTRANET_DAEMON
.acme $U%$H.acme.com@tcp_intranet-daemon
!
```

```
                ! tcp_local
                </etc/opt/SUNWmail/imta//internet.rules

                . $E$U%$H@tcp-daemon
                !
                ...........
                !Channel definitions
                ...........

                !
                ! tcp_intranet
One line: -->   tcp_intranet smtp single_sys subdirs 20 copywarnpost copysendpost
          -->   postheadonly immnonurgent noreverse logging notices 1 2 4 7
                tcp_intranet-daemon mailserver.acme.com

                !
                ! tcp_local
One line: -->   tcp_local smtp single_sys copywarnpost copysendpost postheadonly
          -->   switchchannel subdirs 20 immnonurgent logging notices 1 2 4 7
          -->   remotehost inner
                tcp-daemon mailserver.acme.com

                !
                ..........
```

By adding the noreverse keyword to the `tcp_intranet` channel, address reversal is not done for internal mail. But for the `tcp_local` channel, address reversal (transforming internal addresses to external presentation addresses on messages outgoing to the external world) is performed, since reverse is the default setting for an MTA channel.

The `remotehost` channel keywords is used on the `tcp_local` channel. The `remotehost` and `noremotehost` channel keywords affect the IMTA's handling of bare usernames ("addresses" that are illegally formatted in that they have no domain name). The IMTA always inserts a domain name on such addresses, to make the addresses syntactically legal. The remotehost channel keyword on the `tcp_internet` channel (handling incoming messages from external sites) tells the IMTA to use the remote sending system's (as determined by a reverse DNS lookup); the default `noremotehost` channel keyword on the tcp_internet channel (handling incoming messages from internal sites) tells the IMTA to use its own local host name.

The inner keyword causes the IMTA address rewriting to be applied to addresses in embedded message parts (MESSAGE/RFC822 parts) within the message; if you are applying address reversal on outgoing messages, this is liable to be desirable.

Restricting or Controlling Published Information

- "Restricting SMTP Probe Commands" on page 150
- "Removing Internal Names in Received Headers" on page 151

This section describes various ways information that you might not wish to publish can leak out and describes ways of blocking this.

Restricting SMTP Probe Commands

During an SMTP connection, a remote sending side (or a person manually telnetting to your SMTP port) can issue commands requesting information such as a check on the validity of addresses. This very useful information can, however, be subject to abuse, for example, by automated search engines checking for valid email addresses on your firewall system. Therefore some sites may have an interest in disabling these helpful features. Refer to section on SMTP Channel Option Files in the *SIMS Reference Manual*.

Setting `DISABLE_EXPAND=1` in your Internet TCP/IP channel option file disables the SMTP `EXPN` command. The SMTP `EXPN` command is normally used to expand (get the membership of) mailing lists.

Setting `HIDE_VERIFY=1` in your Internet TCP/IP channel option file causes the IMTA to return a "generic" response to the SMTP `VRFY` command. The SMTP `VRFY` command is normally used to check whether an address is a legitimate address on the local system. (Note that because it is required that SMTP servers support the `VRFY` command, the IMTA has to return some sort of response; with `HIDE_VERIFY=1`, this response is simply a "maybe" sort of response rather than an explicit yes or no.)

Setting `DISABLE_ADDRESS=1` in your Internet TCP/IP channel option file causes the IMTA to disable responses to the IMTA's private `XADR` command, which normally returns information about the channel an address matches.

Setting `DISABLE_STATUS=1` in your Internet TCP/IP channel option file causes the IMTA to disable responses to the IMTA's private `XSTA` command, which normally returns information about the numbers of messages in IMTA queues.

Setting DISABLE_GENERAL=1 in your Internet TCP/IP channel option file causes the IMTA to disable responses to the IMTA's private XGEN command, which normally returns status information about whether an IMTA compiled configuration and character set are in use.

A sample TCP/IP channel option file to disable probing via the SMTP server, for a site using a tcp_local channel, would be as shown in the following example.

```
DISABLE_EXPAND=1
HIDE_VERIFY=1
DISABLE_ADDRESS=1
DISABLE_STATUS=1
DISABLE_GENERAL=1
```

Removing Internal Names in Received Headers

Received headers are normally exceptionally useful headers for displaying the routing that a message really took. Their worth is apparent in cases of dealing with what appears to be forged email, or in cases where you are trying to track down what happened to a broken message, or in cases where a message does not appear to be replyable and you are trying to figure out who might know how to respond to the message. Received headers are also used by the IMTA and other mailers to try to detect message loops.

Message-id headers are normally useful for message tracking and correlation.

However, on the converse side, Received headers on messages you send out give the message recipient information about the routing that a message really took through your internal systems and tend to include internal system names and possibly an envelope recipient address. Also, Message-id headers tend to include internal system names. At some sites, this may be considered a security exposure.

If your site is concerned about this information being published, first see if you can configure your internal systems to control what information they put in these headers. For instance, the IMTA options RECEIVED_DOMAIN and ID_DOMAIN can be used on an IMTA system to specify the domain name to use when constructing Received headers and Message-id headers, respectively. Although these options are not usually particularly relevant on the IMTA firewall system itself—the firewall system is by definition a system whose name is intended to be visible to the outside world—if you have the IMTA on internal systems also, the options may be of interest on those internal IMTA systems. In a similar spirit, the channel keyword noreceivedfor can be used on channels on an IMTA system to instruct the IMTA not to include the envelope recipient address in the Received header it constructs, if limiting the exposure of internal “routing” addresses is a concern for your site. Only if you cannot configure your internal systems to control such sorts of information should you consider resorting to stripping off such headers entirely.

`Received` and `Message-id` headers should not be removed lightly due to their many and important uses, but if the internal routing and system name information in them is sensitive for your site and if you cannot configure your internal systems to control what information appears in these headers, then you may wish to strip off those headers on messages going out to the Internet via header trimming on your outgoing TCP/IP channel.

Note – Do not remove `Received` or `Message-id` headers on general principles or because your users do not like them. Removing such headers (1) removes one of the best tracking mechanisms you have, (2) removes information that may be critical in tracking down and solving problems, (3) removes one of the few (and best) warnings of forged mail you may have, and (4) blocks the mail system's ability to detect and short-circuit message loops. Only remove such headers if you know your site needs them removed.

To implement header trimming, put the `headertrim` keyword—you will probably want the `innertrim` keyword as well—on your outgoing external TCP/IP channel or channels, generally `tcp_local` and possibly other `tcp_*` channels (possibly every `tcp_*` channel except your internal channel, `tcp_internet`), where the x depends upon the TCP/IP package you are using, and create a header trimming file for each such channel. The headertrim keyword causes header trimming to be applied to the outer message headers; the `innertrim` keyword causes the header trimming to be applied also to embedded message parts (MESSAGE/RFC822 parts) within the message. A sample header trimming file for a site using a `tcp_local` channel is shown in the following example.

```
Received: MAXIMUM=-1
MR-Received: MAXIMUM=-1
X400-Received: MAXIMUM=-1
Message-id: MAXIMUM=-1
```

Controlling External Stimulation of Message Delivery

The extended SMTP command ETRN (RFC 1985) allows an SMTP client to request that a remote SMTP server start up processing of the remote side's message queues destined for sending to the original SMTP client; that is, it allows an SMTP client and SMTP server to negotiate "switching roles," where the side originally the sender becomes the receiver, and the side originally the receiver becomes the sender. Or in other words, ETRN provides a way to implement "polling" of remote SMTP systems for messages incoming to one's own system. This can be useful for systems that only have transient connections between each other, for instance, over dial-up lines. When the connection is brought up and one side sends to the other, via the ETRN command the SMTP client can also tell the remote side that it should now try to deliver any messages that need to travel in the reverse direction.

The SMTP client specifies on the SMTP ETRN command line the name of the system to which to send messages (generally the SMTP client system's own name). If the remote SMTP server supports the ETRN command, it will trigger execution of a separate process to connect back to the named system and send any messages awaiting delivery for that named system.

See also Channel Configuration Keywords section in the *SIMS Reference Manual* for a discussion on the channel keywords that affect the IMTA sending and behavior upon receipt of ETRN commands.

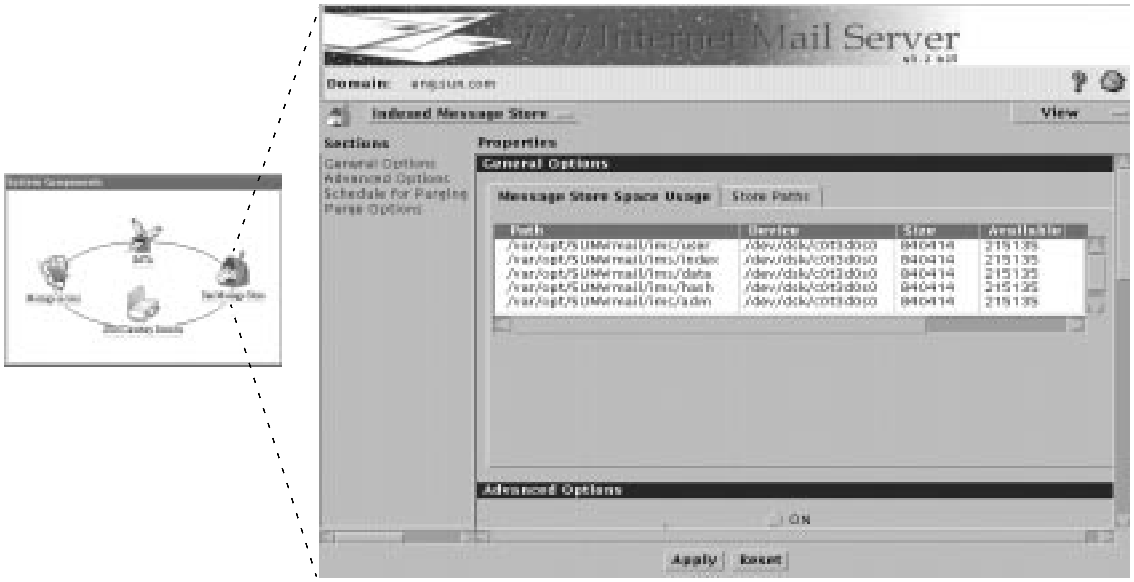
The ETRN command may be quite useful on an e-mail firewall system, particularly if communication partners have only dial-up or other intermittently scheduled connectivity. But for general external SMTP connections, you may wish to limit the number of ETRN commands to which the IMTA will respond in a single session, so that a single remote site cannot attempt to "monopolize" the IMTA system's message delivery processing. For this, the `ALLOW_ETRNS_PER_SESSION` channel option may be used in the external TCP/IP channel's option file.

Also, in the interest of limiting the amount of information about the firewall's configuration visible externally, you may wish to block the IMTA's normal echo of the name of the IMTA channel an ETRN command domain matches on the `tcp_internet` channel handling general external SMTP connections. For this, specify the `silentetrn` channel keyword on the `tcp_internet` channel.

CHAPTER 7

Message Store Administration

This chapter describes step-by-step instructions for changing the Sun Message Store characteristics of the Sun Internet Mail Server (SIMS). To start, bring up the Sun Message Store property book pages.



Path	Device	Size	Available
/var/opt/SUNWmail/ims/user	/dev/dsk/c0t3d0s0	840414	215135
/var/opt/SUNWmail/ims/index	/dev/dsk/c0t3d0s0	840414	215135
/var/opt/SUNWmail/ims/data	/dev/dsk/c0t3d0s0	840414	215135
/var/opt/SUNWmail/ims/hash	/dev/dsk/c0t3d0s0	840414	215135
/var/opt/SUNWmail/ims/adm	/dev/dsk/c0t3d0s0	840414	215135

FIGURE 7-1 Sun Message Store Property Book

Sun Message Store Topics and Tasks

TABLE 7-1 Message Store Topics and Tasks

Topic/Task	Description	Page
Enabling APOP	Encoded password for POP connections.	157
Enabling POP Before SMTP	POP3 login required before messages can be sent via SMTP.	157
Message Store Support for Failover LDAP Hosts	How to configure failover LDAP hosts for the message store.	157
Message Store Configuration Backup and Restore	Back up and restore configuration of the message store.	158
Monitoring the Sun Message Store	Describes how to view the SIMS message store path, space usage, and user space quotas.	160
Message Store Quotas	Describes the SIMS user message store quota system.	162
Configuring Advanced Options	Describes the following: - User quota enforcement/default message quota - Disable or enable proxy server - Setup proxy server capabilities - Mail server client type - Maximum connections permitted - Percentage space left warning threshold - /var/mail support - Size by which to increase Sun Message Store - Message purge options and scheduling	167
Message Purge	Discusses how to configure message purge options and purge schedules.	172
Message Access Protocol Connections	How to view and monitor all user connections to SIMS, as well as start and stop client access to the message store	176
Sun Message Store Maintenance	This section is in Chapter 11, “SIMS Periodic Maintenance Procedures.” It describes the following Sun Message Store maintenance procedures: - Recommended Maintenance Schedule - Message Purge - Message Store Backup and Restore - Message Store Data Check - Importing /var/mail Users - Deleting Old Messages - Deleting the User	234
Message Access Protocols Error Messages	Error messages and proper responses. Appendix D, “Error Messages.”	342

Enabling APOP

Utility: `apop`

APOP is a POP command that the mail client can use as an alternative to USER/PASS (RFC 1939). Unlike USER/PASS, APOP does not use the user's plaintext password for authentication. It instead uses an encoding of the password together with a challenge string. For instructions on how to enable APOP on the server see the man page.

Note that if APOP is not enabled, server will respond with `Err not supported`, if asked to do APOP. To authenticate a user with APOP, their password must be available in plaintext. If it isn't then the authentication will not succeed and they will have to login using the USER/PASS sequence. For instructions on how to enable this feature, refer to the `apop` man page.

Enabling POP Before SMTP

Utility: `popb4smtp`

POP before SMTP (`popb4smtp`) is a mechanism for allowing only users who successfully log in to a POP3 account to send messages via SMTP. `popb4smtp` is useful for preventing the sending of Unsolicited Bulk Email (UBE) through anonymous SMTP connections. For instructions on how to enable this feature, refer to the `popb4smtp` man page.

Message Store Support for Failover LDAP Hosts

The message store uses the LDAP directory to authenticate users logging onto the system to access their mailboxes. The name of the LDAP server used for authentication is specified with the `ims-ldap-server` parameter in the `/etc/opt/SUNWmail/ims/ims.cnf` file. If no value is specified, the default is the local host.

You can also specify failover directory servers for the message store. If one LDAP host is not working, the message store will try the next LDAP host. The following line from the ims.cnf file shows how to specify multiple LDAP failover hosts:

```
ims-ldap-server:host1, host2, host3
```

host1, host2, host3 are the failover LDAP hosts. You can also specify a port number corresponding to a failover LDAP host as follows:

```
ims-ldap-server:host1, host2:port2, host3:port3
```

If no port is specified, the default port of 389 is used. Make sure that the LDAP server on each of these hosts is listening to the specified port.

Two ims.cnf timeout parameters are associated with the LDAP server failover feature:

- ims-ldap-failover-timeout - Number of seconds to successfully bind to a given LDAP server before trying the next server on the list. The default value is 30 seconds.
- ims-ldap-request-timeout - Cumulative number of seconds to successfully open and bind to at least one of the LDAP servers before generating an error message. This value is also the timeout for doing an ldap_search(). The default value is 60 seconds.

Message Store Configuration Backup and Restore

After SIMS is installed and you have responded to prompts for various information during the initial setup of the server, the server saves or *backs up* the Sun Message Store configuration. This configuration version is known as the *default configuration*.

Subsequently, the Admin Console enables you to back up your Sun Message Store configuration at any time. The Admin Console enables you to save up to two versions of the Sun Message Store configuration. The latest working configuration is known as the *current configuration*. The previously saved working configuration is known as the *backup configuration*.

For example, imagine that you reconfigure certain aspects of the Sun Message Store using the Admin Console. You decide to back up this particular configuration on May 1. Because this configuration is the latest working configuration, it is considered the current configuration. On June 1, you reconfigure more aspects of the Sun Message Store and perform another backup. The May 1 configuration becomes the backup configuration and the June 1 configuration is considered the current configuration. On August 1, you reconfigure even more aspects of the Sun Message Store and perform another backup. Because the Sun Message Store can save only two configuration versions, the May 1 configuration is not saved. The June 1 configuration becomes the backup configuration and the August 1 is considered the current configuration.

If for some reason you wish to use a previous Sun Message Store configuration version, you can restore one of the following configuration versions:

- Default configuration
- Backup configuration (provided that this version exists)

▼ To Back Up and Restore the Sun Message Store Configuration

AdminConsole>Sun Message Store Pulldown>Backup config

1. **From the Sun Message Store property book, click the Sun Message Store pull-down menu and select Backup Config.**

   The Sun Message Store makes a backup of the current configuration.

2. **If desired, restore either the default configuration or the backup configuration, if this version exists.**

   a. **To restore the default configuration, click the Sun Message Store pull-down menu and select Use Default Configuration.**

   The Sun Message Store restores the default configuration.

   b. **To restore the backup configuration, click the Sun Message Store pull-down menu and select Use Backup Configuration.**

   The Sun Message Store restores the backup configuration.

Monitoring the Sun Message Store

▼ To Monitor Mail Store Space Usage and Settings

You can monitor the following Sun Message Store parameters:

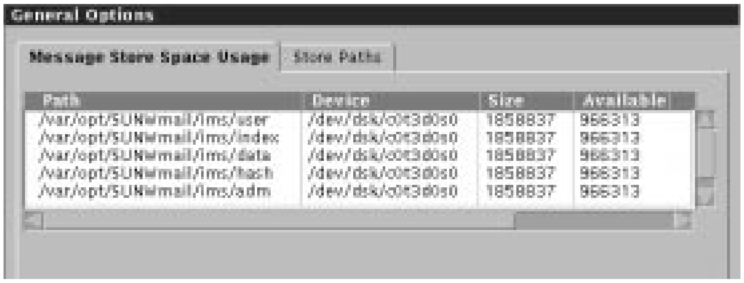
- Current size of the directories that store user folders, indexes, messages and attachments, message hash, Sun Message Store log files, and shared or group folders
- Amount of remaining hard disk space available for each directory listed

AdminConsole>Sun Message Store>General Options>Message Store Space Usage

1. **From the Admin Console home page, click the Sun Message Store icon.**
2. **Click General Options in the Sections list.**

   This section is divided into subsections for the space usage and store paths.
3. **Click the Message Store Space Usage tab.**

   The Message Store Space Usage subsection appears as shown in FIGURE 7-2.



Path	Device	Size	Available
/var/opt/SUNWmail/ims/user	/dev/dsk/c0t3d0s0	1858837	966313
/var/opt/SUNWmail/ims/index	/dev/dsk/c0t3d0s0	1858837	966313
/var/opt/SUNWmail/ims/data	/dev/dsk/c0t3d0s0	1858837	966313
/var/opt/SUNWmail/ims/hash	/dev/dsk/c0t3d0s0	1858837	966313
/var/opt/SUNWmail/ims/adm	/dev/dsk/c0t3d0s0	1858837	966313

FIGURE 7-2 Message Store Space Usage Subsection

- Path - Directory that stores user folders, indexes, messages and attachments, message hash, Sun Message Store log files, and shared or group folders
- Device - Hard disk partition on which the directories reside

- Size - Current size in kilobytes of each directory
- Available - Amount of remaining hard disk space currently available for each directory

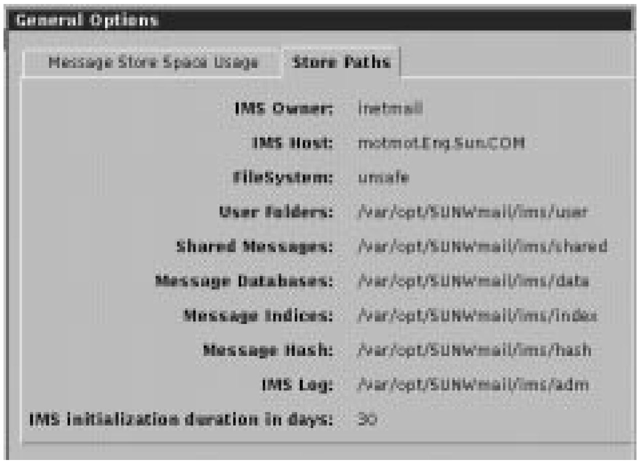
▼ To View Sun Message Store Paths

During SIMS installation, you provided a path name for the directories that store the messages and attachments, indexes, user folders, shared or group folders, message hash, and log file, or you decided to use the default path names. Values for owner, host, and number of days were also assigned during installation. These can be viewed with the following procedure. Of the values displayed in this section, you can reconfigure the number of days to initialize the Sun Message Store only. For more information, refer to “Sun Message Store Increase” on page 169.

AdminConsole>Sun Message Store>General Options> Store Paths

1. **From the Admin Console home page, click the Sun Message Store icon.**
2. **Click General Options in the Sections list.**

   This section is divided into subsections for the space usage and store paths.
3. **Click the Store Paths tab (**FIGURE 7-3**).**



IMS Owner: inetmail

IMS Host: motmot.Eng.Sun.COM

FileSystem: umsafe

User Folders: /var/opt/SUNWmail/ims/user

Shared Messages: /var/opt/SUNWmail/ims/shared

Message Databases: /var/opt/SUNWmail/ims/data

Message Indices: /var/opt/SUNWmail/ims/index

Message Hash: /var/opt/SUNWmail/ims/hash

IMS Log: /var/opt/SUNWmail/ims/adm

IMS initialization duration in days: 30

FIGURE 7-3 Store Paths Subsection

- IMS Owner - Owner (of Sun Message Store files).
- IMS Host - Name of host on which the Sun Message Store is installed.

- FileSystem - This can either be *loggin*g or *nloggin*g. A logging file system performs logging such that if a system crashes it is possible to roll back the data to a pre-crash state and restore all data. An example of a safe file system is VXFS. An nlogging file system does not perform logging. If the system crashes, the state cannot be recreated and some data may be lost. You must also perform an `imcheck` before activating message access to these files.
- User folders - Contains user's email folders.
- Shared Messages - Contains folders for shared folders.
- Message Databases - Contains messages and attachments.
- Message Indices - Contains message index files.
- Message hash - Contains hashing files.
- IMS Log - Sun Message Store log files.
- IMS initialization duration in days - Number of days to initialize the Sun Message Store.

Message Store Quotas

SIMS allows administrators to limit the amount of mail storage allocated to a user. This limit is called the *message store quota*. Once this feature is enabled, the system calculates the amount of disk space occupied by a user's messages. If the amount exceeds the quota specified for that user, further mail is bounced back to the sender and no further mail can be received by this user until the quota is increased or the user deletes some messages in the mailbox. Note that message store quotas can only be used with the Sun Message Store. This feature will not work with `/var/mail`.

SIMS also provides a mechanism to warn users and administrators when their mail store usage approaches their quota. Refer to "To Monitor User Quotas" on page 165.

Note – Quotas can only be set to users and not domains. SIMS provides a mechanism for monitoring the amount of space used by a domain, however, mail to a domain will not be bounced.

Mail Store Usage Calculation

Mail store usage is calculated by totaling the space usage of all the messages in all the user's mailboxes. If a message is sent to multiple users, SIMS adds the message size to the user's total usage—even though the message is only stored in one place with each user having a pointer to it.

▼ To Activate Message Store Quota Enforcement on an Installed System

When SIMS is installed, the message store quota feature is set to `OFF`. This means that user's mailboxes can occupy an unlimited amount of mail storage space. Implementing a message store quota involves the following steps:

1. **Determine how much disk space is available for storing mailboxes and how much space each user can be allocated.**

   As a guideline, the default user message store quota is 20 Mbytes. Change this in the Admin Console's Sun Message Store Property Book ("To Configure Advanced Options" on page 170) or by setting the `ims-default-quota` parameter in the `ims.conf` file to the desired default value.

2. **Set the message store quota for each user entry.**

   See "To Set a User's Mail Store Quota" on page 164.

3. **Shut down the SIMS server.**

   This prevents quota usage inconsistency.

   ```
   # im.server stop
   ```

4. **Activate the message store quota enforcement for the system.**

   Set the `ims-quota` parameter in the `/etc/opt/SUNWmail/ims/ims.conf` file to `on`, or click the User quota enforcement option in the Sun Message Store Property Book-Advanced Options in the Admin console to `ON` (see page 167).

5. **Run `/opt/SUNWmail/ims/sbin/iminitquota -a`.**

   SIMS maintains a quota cache file for each user. This file contains the user's quota and the amount of space currently used. If a user's mailboxes exceed the amount of allocated storage, then further mail sent to the user is bounced back to the sender.

   As described in the above procedure, there is more than one way to enable the various quota options. TABLE 7-2 shows the action required to implement the desired option.

TABLE 7-2 Message Store Quota Option-Action Matrix

Option	Admin Console	ims.cnf	LDAP Directory
Activate SIMS quota checking	Set **User quota enforcement** to `ON` in Sun Message Store Property Book, Advanced Options. (See "To Configure Advanced Options" on page 170)	Set `ims-quota` to `ON`.	Not Available
Set system default quota	Set **Default User quota enforcement** to ON in Sun Message Store Property Book, Advanced Options. (See "To Configure Advanced Options" on page 170)	Set `ims-default-quota` to <size-of-quota-in-bytes>	Not Available
Set user quota	In the user's property book entry select either **Default User Quota**, **No Store Limit**, or **Set Individual Quota**. See "To Modify a User Entry" on page 41)	Not Available	Set MailQuota to -1 (no limit), -2 (default quota) or N (N=quota in bytes)

6. **Restart `imaccessd`.**

```
# im.server start
```

▼ To Set a User's Mail Store Quota

AdminConsole>User Manager>Display then double click the user entry>Mail Information

1. **Bring up the user entry on the SIMS Admin Console.**

   See "To Find and View User/Group Entries" on page 38.

2. **Set the mail store quota in the Mail Information section.**

   This can be done by either setting the LDAP attribute `MailQuota` to one of three values, or setting the quota to one of three options in the user's entry (see "To Modify a User Entry" on page 41, Step 9b for details). The options are:

- Use Default User Quota - This option allocates the amount of storage specified in the Default User Quota set in the Message Store Property Book. (`MailQuota` = -2. If there no `MailQuota` attribute, the system defaults to -2).
- No Store Limit - This turns off the message quota feature giving this user unlimited message store space. (`MailQuota` = -1)
- Set Individual Quota - Select a number and the unit of measure (kilobytes or megabytes). This quota will not take effect until an incremental or full directory synchronization occurs (see "Alias Synchronization Schedule" on page 87 or see the `dirsync`, `iminitquota`, and `imquotacheck` man pages for more information). `MailQuota` = <*Size of Quota in Bytes*>.

The default is `MailQuota` = -2, Use Default User Quota. For information on how to modify the LDAP directory see the *SIMS Provisioning Guide*.

3. **Quota takes effect after the next incremental directory synchronization.**

   See "Alias Synchronization Schedule" on page 87. If you don't want to wait for the next synchronization, you can activate quota enforcement immediately for a user by using the `iminitquota -u <username>` command.

▼ To Monitor User Quotas

Utility: `imquotacheck`

SIMS allows you to monitor the amount of disk space used by individual email users as well as domains using the `imquotacheck` command. You can also automatically send warning message to users whose space usage is approaching their message storage quota. Refer to the man page for further details.

Use `imquotacheck -v` (verbose)

The User Quota page displays as follows:

```
---------------------------------------------------------------------------
Domain         :  eng.sun.com
Max Mailboxes  :  NO LIMIT
---------------------------------------------------------------------------
      Username      |    Quota(byte)  |    Total(byte)  | % used | Status
--------------------+-----------------+-----------------+--------+---------
siteadmin           |        NO LIMIT |               0 |  NA    | NORMAL
deladmin            |        NO LIMIT |               0 |  NA    | NORMAL
boverby             |        20000000 |            3069 | >0%    | NORMAL
katho               |        NO LIMIT |       138269718 |  NA    | NORMAL
davidx              |        20000000 |         7879082 | >39%   | NORMAL
gherman             |        20000000 |        19999820 | >99%   | ALERT
mcintosh            |               0 |        35662057 | >100%  | ALERT
mfang               |        NO LIMIT |        21967034 |  NA    | NORMAL
---------------------------------------------------------------------------
Total Usage for eng.sun.com : 223780780 Bytes
---------------------------------------------------------------------------
```

- User name - Name of each Sun Message Store user sorted alphabetically. Use the scroll bars to view the entire list.
- Quota - Maximum amount of hard disk space that can be used in kilobytes.
- Total - Amount of hard disk space used in kilobytes.
- Used - Amount of hard disk space used in percentage.
- Status - ALERT indicates that the user has exceeded 85% of the quota.

▼ To Warn Users When Their Mail Store Usage Is Approaching Their Mail Store Quota

The `imquotacheck` command sends an email warning to users who are approaching their mail store quota. This command can be put in a `cron` file to provide a daily check on mail store users. You can configure the desired warning message using the `-f` flag. See the man page.

▼ Setting Soft Quotas

AdminConsole>Sun Message Store>Advanced Options>User quota enforcement

When a *hard quota* is exceeded, no more messages will be accepted into the message store until the message store size is reduced. To set a hard quota, follow the instructions in “To Activate Message Store Quota Enforcement on an Installed System” on page 163.

When a *soft quota* is exceeded, messages will be accepted into the message store, but a message is generated and sent to the user saying that their quota has been exceeded. To set a soft quota:

1. **Shut down the SIMS server.**

   This prevents quota usage inconsistency.

   ```
   # im.server stop
   ```

2. **Deactivate the message store quota enforcement for the system.**

   Click the User quota enforcement option in the Sun Message Store Property Book-Advanced Options in the Admin Console to `OFF` (see page 167).

3. **Set up a cron job to run** `iminitquota` and `imquotacheck.`

   The following example executes `imquotacheck` on all users (`-a`) at 2:30 every night and sends a report to `quota.out`. `imquotacheck` sends a notification to users who exceed the quota.

   ```
   30 2 * * * iminitquota -a; imquotacheck -v > /var/opt/SUNWmail/
   ims/adm/quota.out
   ```

4. **Restart `imaccessd`.**

   ```
   # im.server start
   ```

Configuring Advanced Options

The following is configurable in the Advanced Options section:

- User quota enforcement/default message quota
- Mail server client type
- Maximum connections permitted
- Warning threshold for percentage space remaining

- `/var/mail` support
- Size by which to increase Sun Message Store
- Purge schedule

The following sections provide background information on each of the options that will help you decide if you want to configure them.

User Quota Enforcement

By default, each SIMS user has no maximum amount of hard disk storage or *quota* that they can use for their mailboxes. They can use an unlimited amount of disk space for their incoming and stored messages. SIMS allows you to configure a quota for each Sun Message Store user. If you decide to implement user quotas, you can set a customized quota for each user, or you can set the default quota for a user. The default quota, which can also be changed, is 20 Mbytes. For complete details see "Message Store Quotas" on page 162.

Mail Server Client Type

The Sun Message Store handles the parsing of messages for Internet Mail Access Protocol version 4 (IMAP4) clients and Post Office Protocol version 3 (POP3) clients in different ways. IMAP4 messages are preparsed and indexed when inserted into the Sun Message Store; no parsing is necessary when messages are accessed by mail client users. POP3 messages do not require parsing; therefore, the Sun Message Store does not parse these messages.

By default, the Sun Message Store treats all messages as messages from IMAP4 clients.

Since parsing takes CPU cycles and creates a need for more hard disk space, you may want to tune the amount of parsing that your mail server performs. If a majority of the messages stored by the Sun Message Store are from POP3 clients, you can change the default setting to POP3. The Sun Message Store will treat all messages as messages from POP3 clients and not parse them.

Maximum Connections Permitted

By default, the maximum number of active connections from IMAP4 clients that the Sun Message Store accepts is 10,000. The Advanced Option section in the Sun Message Store property book enables you to expand the maximum number of connections using the maximum connections permitted option. The up and down arrows for this option allow you to select a value in the range of 50 to 2,000,000,000 (billion).

When raising the maximum number of connections, keep in mind that the Sun Message Store daemons reserve shared memory for interprocess communication based on this number. If too high a number is configured, the Sun Message Store fails to allocate sufficient shared memory to handle the maximum number of connections specified. The Sun Message Store will log an error message and exit.

If you attempt to configure the mail server to accept above the maximum number of connections permitted, `imaccessd` will log a message stating that the maximum connection number was exceeded and that the default number of 10,000 is being enforced.

Warning Threshold for Space Remaining

By default, when the amount of hard disk space for the Sun Message Store is down to 5 percent, you will receive a warning in the System Status section of the Admin Console home page. The Advanced Option section in the Sun Message Store property book enables you to reconfigure the space threshold at which you will be warned.

`/var/mail` Support

By default, access to mailboxes in `/var/mail` is not supported. The Advanced Option section in the Sun Message Store property book enables you to reconfigure this default so that users who have mailboxes in `/var/mail` can access the mailboxes using either the IMAP4 or POP3.

Sun Message Store Increase

The Sun Message Store stores messages using a time-based structure. By default, a data directory contains 30 subdirectories, or one subdirectory for each day of the month. The data directory stores messages and attachments as files. For example, on May 1, all messages that enter the Sun Message Store are stored in the day 1 subdirectory. On May 15, all messages are stored in the day 15 subdirectory.

The Advanced Option section in the Sun Message Store property book enables you to reconfigure the time-based structure in which messages are stored using the Increase Store Size option. For example, if you specify 3 weeks, 21 subdirectories are created, 1 for each day of the 21-day interval. Messages entering the Sun Message Store on the first day of the interval are stored in the day 1 subdirectory and so on.

The distinction between the month and week intervals is that if you specify weeks, the Sun Message Store needs to allocate space more frequently than if you specify months. Modifying this feature has no impact on performance or resources.

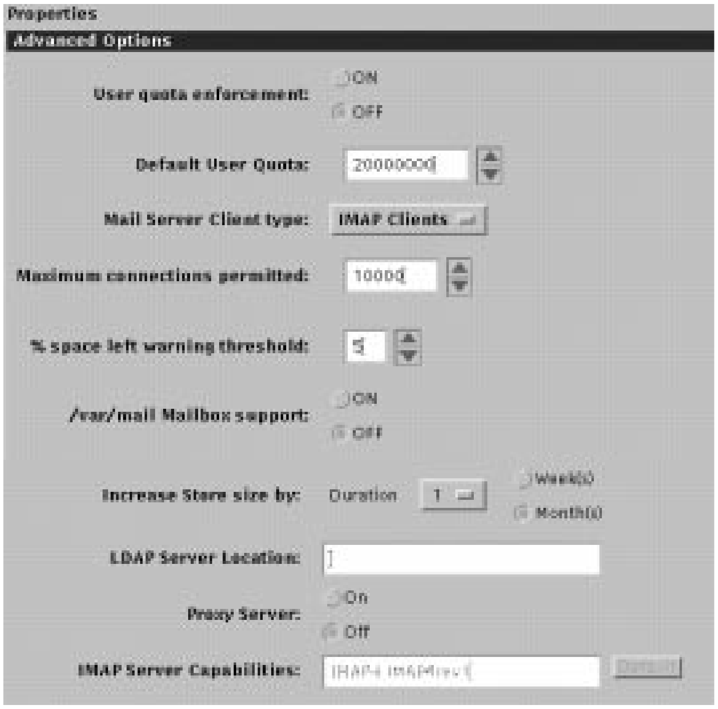
▼ To Configure Advanced Options

Configuring these features is optional.

AdminConsole>Sun Message Store>Advanced Options

1. **From the Admin Console home page, click the Sun Message Store icon.**
2. **Click Advanced Options in the Section list.**

   The Advanced Options section appears, as shown in FIGURE 7-4.



Properties

Advanced Options

User quota enforcement: ○ ON ● OFF

Default User Quota: 20000000

Mail Server Client type: IMAP Clients

Maximum connections permitted: 10000

% space left warning threshold: 5

/var/mail Mailbox support: ○ ON ● OFF

Increase Store size by: Duration 1 ○ Week(s) ● Month(s)

LDAP Server Location:

Proxy Server: ○ On ● Off

IMAP Server Capabilities: IMAP4 IMAP4rev1

FIGURE 7-4 Advanced Options Section (Extended View)

3. **Enable or disable the User Quota Enforcement option.**

   - Click ON to allow user message store space quotas to be set.
   - Click OFF to allow users unlimited message store space.

   See “Message Store Quotas” on page 162 for a complete discussion on user quotas. See “To Modify a User Entry” on page 41, Step 9b for instructions on how to set the message store quota for user entries.

4. **Reconfigure the default message quota by clicking the up or down arrow keys.**

   This is the default quota for new users if the User Quota Enforcement option is set to ON. See “To Modify a User Entry” on page 41, Step 9b, for details on how to set a customized user quota.

5. **To configure how the Sun Message Store handles the parsing of messages from IMAP4 and POP3 clients, click the menu and choose the desired client type.**

   Mail Server Client Type has two choices: POP3 and IMAP4. However, if you set the configuration to IMAP4, the POP3 choice will be removed from the menu. Once IMAP4 client is set, you cannot change back to POP3 in the Admin Console. If the configuration is set to POP3, you can change it to IMAP4 to make the message store parse messages. (You can change from IMAP4 to POP3 if the message store has no data at all. Modify the `ims-parse-level` parameter in the `ims.cnf` file. See the "Message Access and Store Configuration" chapter in the *SIMS Reference Guide*. If the message store has data, you cannot change it.)

6. **Configure the maximum number of connections from IMAP4 clients that the Sun Message Store accepts by clicking the up or down arrows.**

   The valid range includes 50 through 100,000.

7. **Configure the "percentage of space left" warning threshold by clicking the up or down arrow keys.**

8. **Configure `/var/mail` support by clicking the appropriate radio button.**

9. **Configure the time-based structure in which messages are stored by choosing a number from the menu and clicking the radio button associated with the preferred unit of measure.**

10. **Configure the LDAP server host name for the Message Store.**

    Note that the LDAP server for all SIMS components is specified by the `ldapServer` server parameter in the `/etc/opt/SUNWmail/sims.cnf` file. If you want to use a different directory server for the message access / message store, you can specify a different directory server here. However, all other SIMS components will continue to use the server specified by `ldapServer`. If an existing MSMA directory server is specified, for example from previous release, then that directory server is used and will be displayed in this field.

11. **Use the Proxy Server radio buttons and the IMAP Server Capabilities only to configure the server as a SIMS Proxy server.**

    See "Setting Up a Proxy+Mail Server" on page 311.

12. **Click the Apply button.**

Message Purge

When a message is delivered into the Sun Message Store, a reference pointing to the stored message is created in the inbox of each of the message recipients. As each recipient reads, deletes, and removes (expunges) the message via their respective mail clients, the associated reference to the message is removed. When all references are removed or expired (see “Deleting Old Messages” on page 245), the message can be purged from the Sun Message Store.

Purge messages by manually executing the `impurge` command (see the man page) or by using the Admin Console to automatically run `impurge`.

Note – Do **not** wait until your disk is full before doing a message purge. Run a message purge while there is more empty disk space than the amount of space used by the mail store on its busiest 24-hour period. You can roughly calculate mail store disk usage by noting the disk usage increase on the `/var/opt/SUNWmail/ims` partition over a 24-hour period. If your message purge fails due to lack of disk space, refer to “Message Purge Failure” on page 277.

For additional information on Sun Message Store maintenance, including purge, refer to “Sun Message Store Maintenance” on page 234.

Configuring Purge Options

The Admin Console enables you to configure the following purge options:

- Exhaustive purge - Locate all deleted messages that can be purged and purge them. (A deleted message is a message that is no longer referenced by any user or shared folder.)
- Customized purge - Perform daily computations to determine if the amount of deleted messages on a given day exceeds a percentage threshold and if the amount of disk space recovered if a purge is performed exceeds a size threshold.

Purging a message store supporting more than 20,000 users could take hours, so for some systems it may be preferable to choose Customized Purge rather than an Exhaustive Purge since fewer purges will be required. Users can still send and receive mail during a purge, but the system cannot delete or expunge messages until after the purge is completed.

Customized Purge

You can customize a policy whereby the purging of unreferenced or deleted messages from the Sun Message Store is performed on an as-specified basis rather than on a daily basis. The customized purge option enables you to set two thresholds: percentage and size.

Percentage is defined as the fraction of deleted messages of the total volume of messages handled by the Sun Message Store on a particular day. Size is defined as the total amount of disk space in kilobytes that can be recovered after deleted messages are purged. The system computes percentages and sizes that are compared against these thresholds daily.

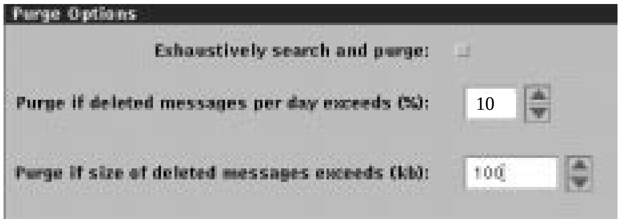
For example, imagine that you have set the percentage threshold to 50 percent and the size threshold to 100 Kbytes. Imagine that on the first day after a purge is performed (day 1), the system examines the total volume of messages handled by the Sun Message Store and the total volume of deleted messages. The system computes the percentage of deleted messages based on the total volume of messages. If the percentage of deleted messages is 51 percent or higher, then day 1 is purged. If the percentage of deleted messages is 50 percent or lower, then day 1 is not purged. Additionally, if the size of deleted messages exceeds 100 Kbytes, then a purge is also performed.

▼ To Configure Purge Options

AdminConsole>Sun Message Store>Purge Options

1. **Click the Sun Message Store icon in the home page.**
2. **Click Purge Options in the Section List.**

   The Purge Options section appears as shown in FIGURE 7-5.



Purge Options

Exhaustively search and purge: □

Purge if deleted messages per day exceeds (%): 10

Purge if size of deleted messages exceeds (kb): 100

FIGURE 7-5 Purge Options Section

3. **If you want to enable the exhaustive purge option, click the associated check box.**
4. **If you want to enable the customized purge option, click the up or down arrow keys to specify the percentage and size thresholds.**

   The default percentage threshold is 1 percent, and the default size threshold is 100 Kbytes.

5. **Click the Apply button.**

▼ To Configure the Purge Schedule

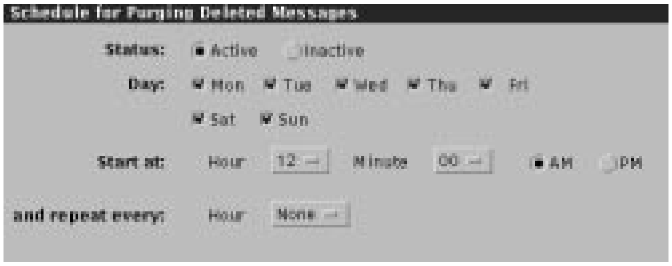
For information on Sun Message Store maintenance, including purge, refer to “Sun Message Store Maintenance” on page 234.

No default purge schedule exists. Therefore, if you want to *purge* or permanently remove messages that no longer have references from any folder on a regularly scheduled basis, you must set a schedule.

AdminConsole>Sun Message Store>Schedule For Purging Deleted Messages

1. **Click the Sun Message Store icon to access the Sun Message Store property book.**
2. **Click Schedule For Purging Deleted Messages in the Sections list.**

   The Schedule For Purging Deleted Messages section appears, as shown in FIGURE 7-6.



Schedule for Purging Deleted Messages

Status: ● Active ○ Inactive

Day: ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri

☑ Sat ☑ Sun

Start at: Hour 12 Minute 00 ● AM ○ PM

and repeat every: Hour None

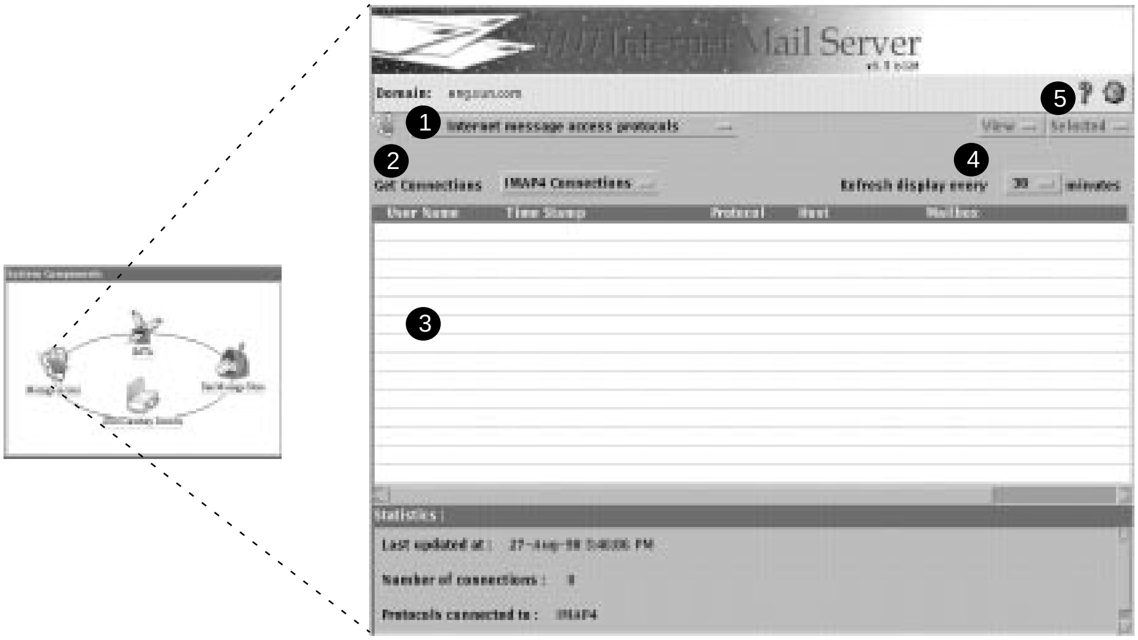
FIGURE 7-6 Schedule For Purging Deleted Messages Section

3. **Activate the purge schedule.**
4. **Configure the purge schedule.**

   Specify days and times at which you want purge to occur.
5. **If you want purge to occur at regularly scheduled intervals throughout the days specified in the purge schedule, specify the interval at which the purge should occur.**
6. **Click the Apply button.**

Message Access Protocol Connections

The Message Access Property Book allows you to view and monitor all user connections to SIMS, as well as start and stop message access to the message store.



Domain: eng.sun.com

Get Connections IMAP4 Connections

Refresh display every 30 minutes

Last updated at : 27-Aug-98 5:40:06 PM

Number of connections : 0

Protocols connected to : IMAP4

FIGURE 7-7 Message Access Property Book

1. **Start message access protocols IMAP4/POP3**
   Stop message access protocols IMAP4/POP3

   Pull-down menu - allows you to start and stop client access to message store. Messages are still received and stored, but clients cannot access the messages.

2. **Get IMAP Connections**
   Get POP3 Connections
   Get Both Connections

   Pulldown menu - specify which user connections to display.

3. **Connections to SIMS**

   A list of all connections to the server by user, time, protocol, host, and open mailbox. The table displays the following fields related to each connection:

   - User Name - User name associated with the connection.
   - Time Stamp - Date and time at which user established connection to mail server.
   - Protocol - Message access protocol used to make connection.
   - Host - Host name of machine from which the connection is made. By default this is the IP address of the host machine. You can change this to be the name of the host machine by changing the `ims-client-lookup` to `DNSON` in `ims.conf`. However, changing to `DNSON` results in the DNS reverse lookup calls made to the DNS server, which can increase the amount of time it takes for clients to login.
   - Mailbox - Mailbox that user is accessing via the connection. A user can access multiple mailboxes at any given time.

   The Statistics area provides the following information:

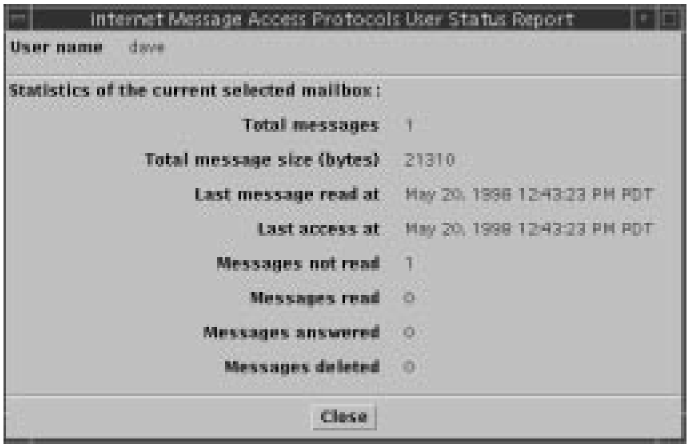
   - Date and time at which the connection table is accessed or updated.
   - Total number of specified connections.
   - Type of connections that you specified.

4. **(Optional) To change the interval at which the connection table is updated (default: 30 minutes), click the Refresh display every X minutes**

   Pull-down menu - Allows you to adjust the frequency of refresh from 30 to 300 minutes.

5. **Get Status**

   Returns status report of highlighted connection. You can also get this report by double-clicking on the preferred connection. The



Internet Message Access Protocols User Status Report

User name dave

Statistics of the current selected mailbox :

Total messages	1
Total message size (bytes)	21310
Last message read at	May 20, 1998 12:43:23 PM PDT
Last access at	May 20, 1998 12:43:23 PM PDT
Messages not read	1
Messages read	0
Messages answered	0
Messages deleted	0

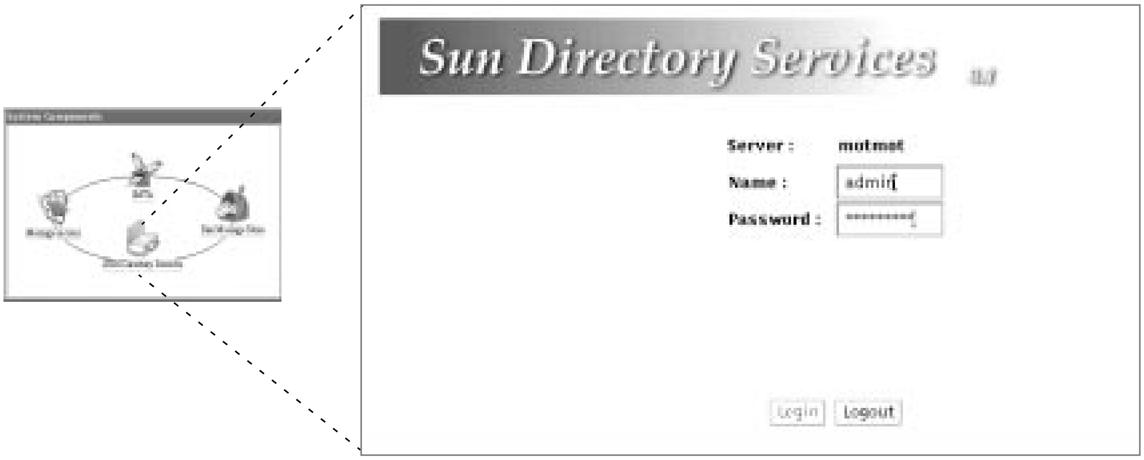
FIGURE 7-8 Connection Status

CHAPTER 8

Sun Directory Services Administration

SIMS supports either the Sun Directory Services and the Netscape Directory Services. The most common directory services tasks are adding, deleting and modifying entries. These are described in Chapter 3, “User/Group Management.” For all other directory service information, refer to the following docs:

- *Sun Directory Services documentation* (http://docs.sun.com:80/ab2/coll.297.1/@Ab2CollToc?subject=sysadmin)
- *Netscape Directory Services documentation* (http://home.netscape.com/eng/server/directory/)



Server : motmot

Name : admin

Password : *********

FIGURE 8-1 Sun Directory Services Property Book

If the Sun Directory Services is installed in your system, you can access its Admin Console by clicking on the icon on the SIMS Admin Console home page. If you have the Netscape Directory Service installed, you will not have a directory service icon at all, and will need to access the Admin Console from the command line.

Note – To log in to the directory service GUI, you need to use the directory administrator's uid and password which may be different from the SIMS Administrator's uid and password.

Sun Directory Services Topics and Tasks

TABLE 8-1 Sun Directory Services Topics and Tasks

Topic/Task	Description	Page
Sun Directory Services 3.1 Administration Guide	http://docs.sun.com:80/ab2/coll.297.1/@Ab2CollToc?subject=sysadmin	
Specifying Current and Backup LDAP Servers for SIMS	Self-explanatory.	180
Starting and Stopping the Sun Directory Services	Self-explanatory.	181
Viewing Sun Directory Services Configuration for SIMS	Describes how to configure the two mandatory parameters: the administrator name/password and the distinguished name of the naming context held in the data store and the data store location.	182
Periodic Maintenance for the Sun Directory Services	This section is in Chapter 11, "SIMS Periodic Maintenance Procedures." It describes: - Maintaining the data store attribute indexes - Backup and restore directory data base - Back up and restoring directory service configuration	246
Troubleshooting the Directory Service	- Diagnosing SIMS Problems Caused by Improper Directory Entries	295

Specifying Current and Backup LDAP Servers for SIMS

SIMS typically uses the directory server installed with the system. It is possible, however, to designate a different directory server to support SIMS. This is done using the `imadmin-modify-currentldap`. Refer to the man page for complete information.

It is also possible to designate backup directory servers in the event that current directory server goes down. Refer to the `imadmin-add-ldapserver` man page for complete information.

Starting and Stopping the Sun Directory Services

You can start the directory server daemon, `dsservd`, from the Sun Directory Services Admin Console, or you can start the directory server daemon by typing the following command as `root`:

```
# /etc/init.d/dsservd start
```

If you change the directory service configuration, you can restart `dsservd` without dropping the connections to current LDAP clients. In this case use the dsservd restart command:

```
# /etc/init.d/dsservd restart
```

You can stop the daemon from the Sun Directory Services Admin Console, or you can stop the directory server daemon by typing the following command as `root`:

```
# /etc/init.d/dsservd stop
```

Stopping the directory server automatically stops the replication server. If you have set up a replication schedule, the replication server is restarted automatically when you restart the directory server, and will continue to follow the schedule.

Viewing Sun Directory Services Configuration for SIMS

When SIMS is installed, the Sun Directory Services are given default configuration settings, which in most cases will not need to be modified. This section describes the Sun Directory Services configuration settings that relate to SIMS (other settings will not be described). For more details, refer to the *Sun Directory Services 3.1 Administration Guide*.

General Properties Configuration

The basic settings are accessible through the Sun Directory Services Admin Console, an expanded version of which is shown in FIGURE 8-2, FIGURE 8-3, and FIGURE 8-4. The following bulleted items describe the settings starting from the top of the console and going down. Only settings relevant to SIMS are described.

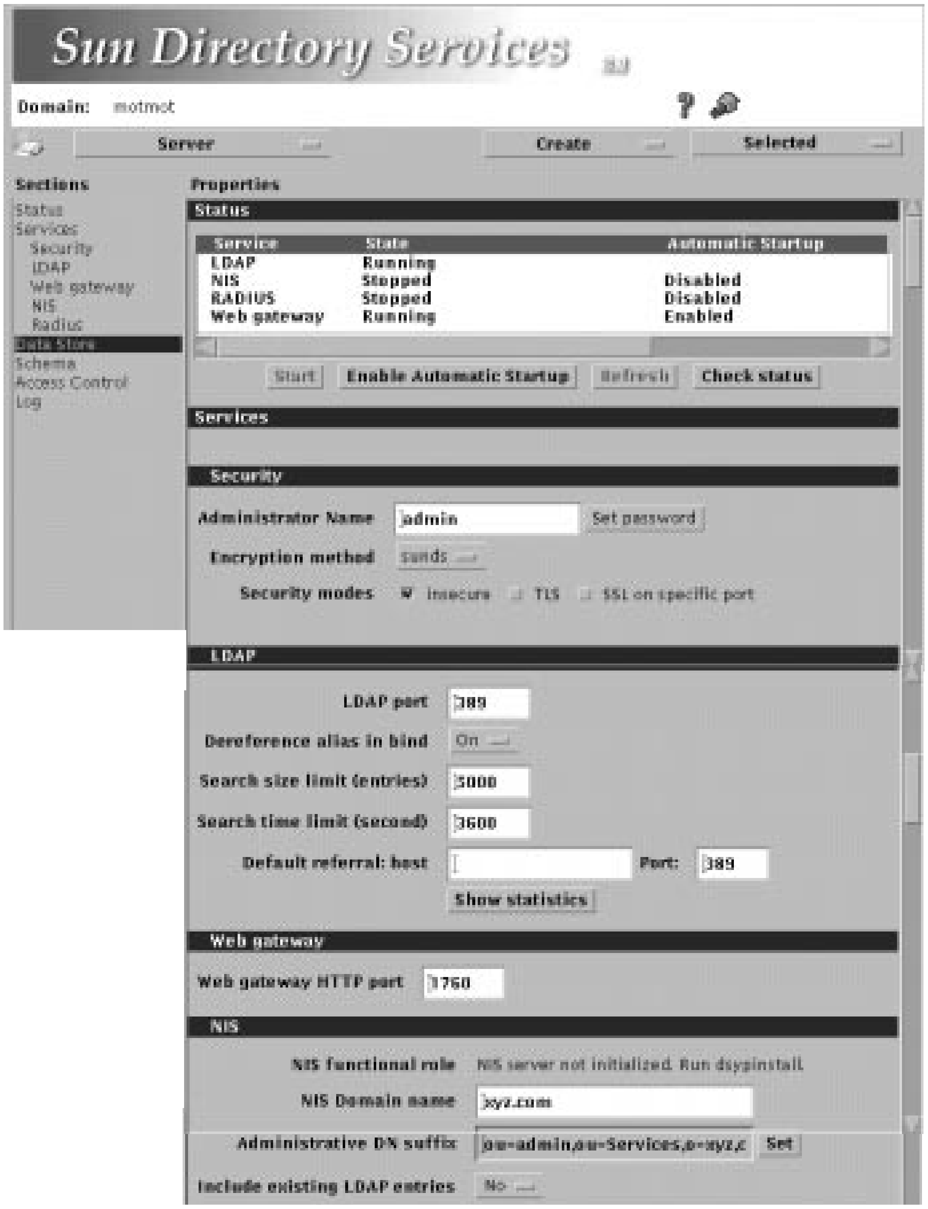
- **Status** shows the status of the supported services. Only LDAP must be running for SIMS to operate.
- **Security** allows you to set the name and password to access Sun Directory Services Admin Console.
- **LDAP** has several different parameters:
  - **LDAP port** shows the port on which the server listens for incoming SIMS requests. Default: 389.

    If you change the LDAP port, the IMTA directory synchronization will not work unless you change the parameter `IMTA_LDAP_SERVER` in `/etc/opt/SUNWmail/imta/imta_tailor` to the new LDAP port value for this particular server. For example, if the LDAP port number is changed from 389 to 390, then change the entry from `xxx.eng.bridge.com:389` to `xxx.eng.bridge.com:390`.
  - **Search size limit** and **Search time limit** specifies the limits for LDAP searches of SIMS entries. A search stops when the first of these is reached. If there are several million entries, a complex search could exceed either of these limits. The default is 5000 entries or 3600 seconds (1 hour).
  - **Default referral host** specifies the default directory server for referrals. Default: None.
- **Data Store** shows a map of the SIMS naming contexts and replicas. Data stores naming contexts, and replicas can be created and modified. See “Data Store Configuration Settings” on page 186

- **Schema** displays the overall LDAP schema of which the SIMS schema is a subset. Also displayed is the schema checking. Default: Weak (schema is checked for each add/modify directory operation).
- **Access Control** displays the access properties for specified SIMS entries. During SIMS installation an access control rule is added for the SIMS Administration.

Warning – Making changes to the SIMS access control could expose data to unauthorized users. The default access control rules are adequate for most uses.

- **Log** shows various LDAP logging information. Logging information may be useful if you are diagnosing LDAP problems. Default: `/var/opt/SUNWconn/ldap/log.`



Domain: motmot

Service	State	Automatic Startup
LDAP	Running	
NIS	Stopped	Disabled
RADIUS	Stopped	Disabled
Web gateway	Running	Enabled

Administrator Name: admin

Encryption method: sunds

Security modes: ☑ insecure □ TLS □ SSL on specific port

LDAP port: 389

Dereference alias in bind: On

Search size limit (entries): 5000

Search time limit (second): 3600

Default referral: host Port: 389

Web gateway HTTP port: 1760

NIS functional role: NIS server not initialized. Run dsypinstall.

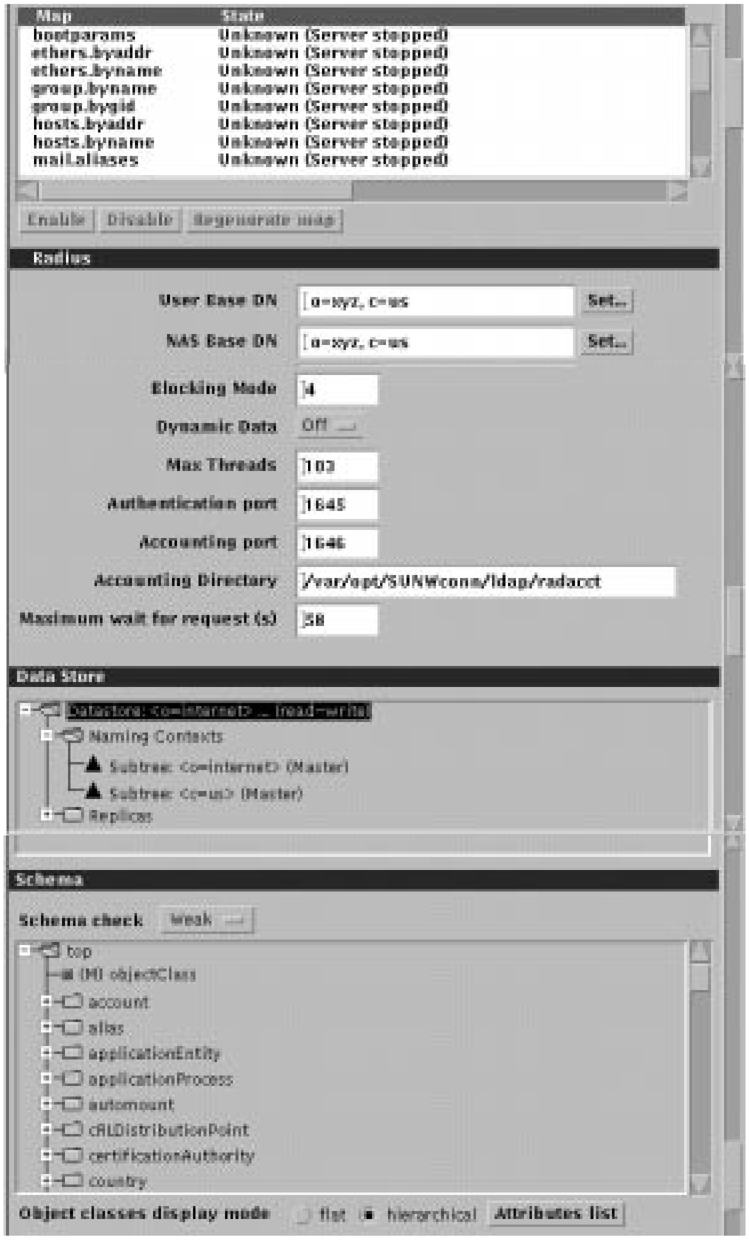
NIS Domain name: xyz.com

Administrative DN suffix: ou=admin,ou=Services,o=xyz,c

Include existing LDAP entries: No

•
•
•

FIGURE 8-2 Sun Directory Services Admin Console Extended View (Page 1 of 3)



Map	State
bootparams	Unknown (Server stopped)
ethers.byaddr	Unknown (Server stopped)
ethers.byname	Unknown (Server stopped)
group.byname	Unknown (Server stopped)
group.bygid	Unknown (Server stopped)
hosts.byaddr	Unknown (Server stopped)
hosts.byname	Unknown (Server stopped)
mail.aliases	Unknown (Server stopped)

User Base DN	o=xyz, c=us
NAS Base DN	o=xyz, c=us
Blocking Mode	4
Dynamic Data	Off
Max Threads	103
Authentication port	1645
Accounting port	1646
Accounting Directory	/var/opt/SUNWconn/ldap/radacct
Maximum wait for request (s)	58

Datastore: <o=internet> ... (read-write)
Naming Contexts
Subtree: <o=internet> (Master)
Subtree: <c=us> (Master)
Replicas

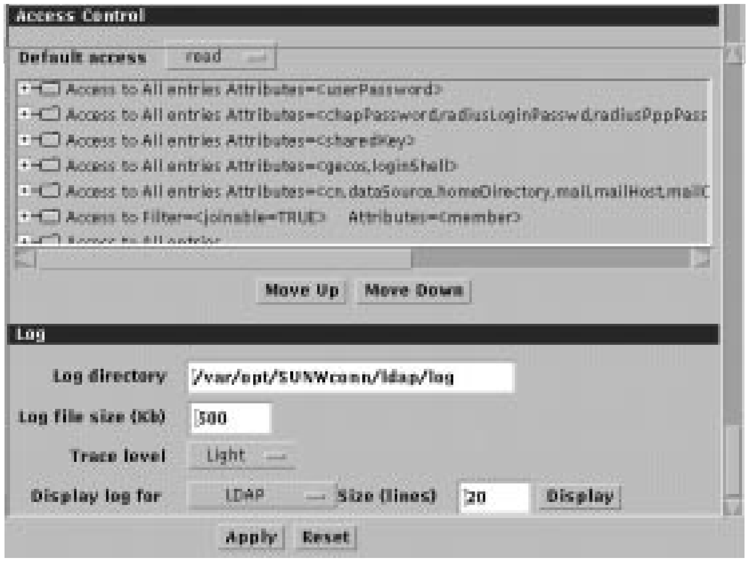
Schema check Weak

top
(M) objectClass
account
alias
applicationEntity
applicationProcess
automount
cRLDistributionPoint
certificationAuthority
country

Object classes display mode ○ flat ● hierarchical

•
•
•

FIGURE 8-3 Sun Directory Services Admin Console Extended View (Page 2 of 3)



Default access: read

- Access to All entries Attributes=<userPassword>
- Access to All entries Attributes=<chapPassword,radiusLoginPasswd,radiusPppPass
- Access to All entries Attributes=<sharedKey>
- Access to All entries Attributes=<gecos,loginShell>
- Access to All entries Attributes=<cn,dataSource,homeDirectory,mail,mailHost,mailC
- Access to Filter=<joinable=TRUE> Attributes=<member>
- Access to All entries

Log directory: /var/opt/SUNWconn/ldap/log

Log file size (Kb): 500

Trace level: Light

Display log for: LDAP Size (lines): 20

FIGURE 8-4 Sun Directory Services Admin Console Extended View (Page 3 of 3)

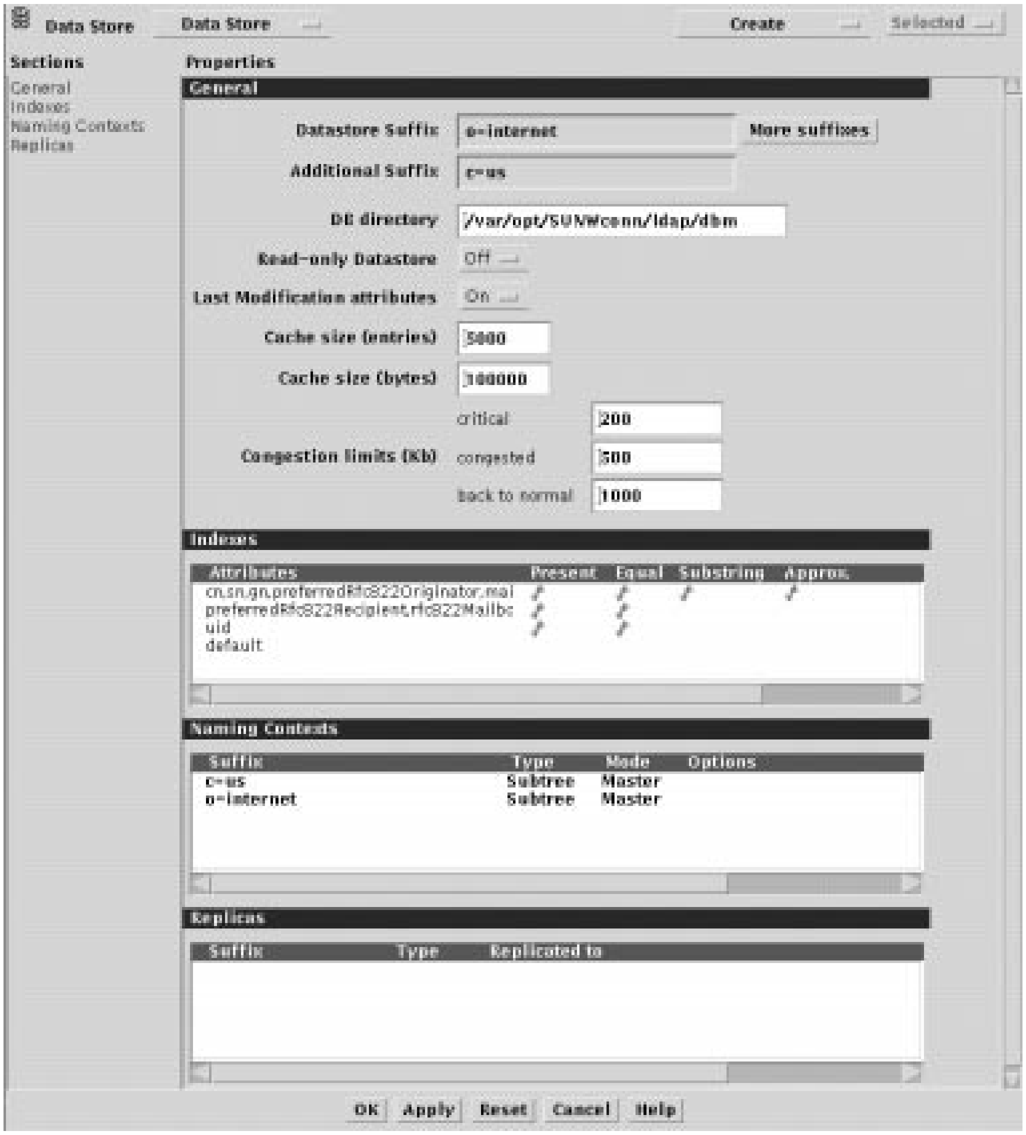
Data Store Configuration Settings

The data store refers to the physical storage space for SIMS LDAP data (essentially user and group entries). For many environments, the data store configured at installation is adequate, however, you may wish to modify or access the data store configuration for the following purposes:

- **Backing up the SIMS data store**. The Sun Directory Services Admin Console displays the file space containing the data store.
- **To view or modify the indexed entry attributes**. Indexing optimizes searches for entries by attribute.
- **To view the naming contexts stored in the data store**.
- **To view the replicas supported by the directory service**.

This section describes the data store configuration settings as they relate to SIMS. These setting are viewable from the Sun Directory Services Admin Console (FIGURE 8-5). For additional conceptual information refer to the *SIMS Concepts Guide*. For additional information on configurable data store settings, as well as how to create or modifying data stores see the *Sun Directory Services 3.1 Administration Guide*.

- **Datastore Suffix** is a naming context contained in the datastore. A data store can have up to four naming contexts. Separate naming contexts might be used to store separate domains.
- **DB Directory** refers to the file space containing the SIMS data store. Default: `/var/opt/SUNWconn/ldap/dbm.`
- **Indexes lists the attributes that are indexed and by what rules they are indexed. Indexing optimizes SIMS entry searches. Any attribute that will be searched should be indexed. The most commonly searched attributes are indexed upon SIMS installation:**
- **Naming Contexts** shows SIMS naming contexts in the datastore as well as their type (object or subtree) and the mode (master or slave). Master means that this naming context contains the master list of entries. Slave means that this naming context is a replicated copy of the master list of entries.
- **Replica** shows the replicated copies of the naming contexts, and what hosts to which they are replicated. Replication is most commonly used in SIMS message access proxies.



General

Datastore Suffix: o=internet

Additional Suffix: c=us

DB directory: /var/opt/SUNWconn/ldap/dbm

Read-only Datastore: Off

Last Modification attributes: On

Cache size (entries): 5000

Cache size (bytes): 100000

Congestion limits (Kb): critical 200; congested 500; back to normal 1000

Indexes

Attributes	Present	Equal	Substring	Approx.
cn,sn,gn,preferredRfc822Originator,mai	✓	✓	✓	✓
preferredRfc822Recipient,rfc822Mailbo	✓	✓		
uid	✓	✓		
default				

Naming Contexts

Suffix	Type	Mode	Options
c=us	Subtree	Master	
o=internet	Subtree	Master	

Replicas

Suffix	Type	Replicated to

FIGURE 8-5 Data Store Configuration.

CHAPTER **9**

Populating SIMS with Users and Groups

This chapter describes how to populate users and groups from your current directory database to the SIMS directory.

Users and groups can be manually entered into the SIMS system using the `imadmin-add-user` command or the SIMS Admin Console (see “To Create a User Entry” on page 28), or by modifying the directory. However, it may be easier to migrate users from an existing directory database to the SIMS directory. If the directory from which you wish to populate users and groups is NIS, NIS+, or `/etc` files, then we provide a defined procedure and scripts to do this. However, If the directory from which you wish to populate users and groups is in a database other than NIS, NIS+, or `/etc` files, then you will have to extract the desired data from your current directory and put it into the SIMS LDAP directory. This is a process known as provisioning. See the *SIMS Provisioning Guide* for complete information on this topic. See the *SIMS Reference Manual* for the SIMS schema.

The remainder of this chapter describes how to populate users and groups from NIS, NIS+, or `/etc` files.

This chapter does not describe how to migrate user mailboxes from existing mail systems into SIMS. This information is described in Chapter 9, “Populating SIMS with Users and Groups.”

Populating the Directory from NIS, NIS+, or /etc Files Entries

This section describes two ways in which to populate the directory with entries for mail users, user aliases, and distribution lists.

1. Writing LDIF data directly into the LDBM database using `ldif2ldbm` and bypassing the `dsservd` server. This is a fast way of doing bulk loading. However, there is no schema checking done with this method. Use this method only if you are certain that your LDIF data is compliant with the schema supported by your `dsservd` server.
2. Populating the directory via the `dsservd` server. This is a safer, but more time-consuming way of populating the directory using the LDAP protocol.

Note – By default SIMS assumes that all users receiving mail on this server have entries in the LDAP Directory. Mail will not be routed to users by SIMS until the LDAP Directory is populated with entries. SIMS can be configured to forward unroutable mail to a DNS “smarthost”; see “To Configure IMTA Position Relative to the Internet” on page 91 if you wish mail to be forwarded to the smarthost in the event the intended recipient is not in the LDAP Directory.

Directory entries are created from the `passwd(4)` file and the mail `aliases(4)` file. These procedures describe populating the directory for use by SIMS, not for general purpose directory use. “Populating the directory” in this scope means “adding User and Alias entries to the directory for use by SIMS.” Other attributes may be added to the directory for other uses, but they must not interfere with the attribute/value pairs used by SIMS.

For a look at some sample directory population sessions, refer to “Populating the Directory with User Data—Sample Session” on page 321, “Populating the Directory with User Aliases Data and Distribution Lists —Sample Session” on page 325, and “Populating the Directory with User Aliases Data and Distribution Lists —Sample Session” on page 325.

Setting the Environment for Directory Population

These procedures use many different commands and several different configuration files. Add the paths to these commands to your own shell paths or `$MANPATH`.

- Executable programs and scripts:

```
/opt/SUNWmail/bin
/opt/SUNWmail/sbin
/opt/SUNWconn/bin
/opt/SUNWconn/sbin
```

- Directory man pages:

```
/opt/SUNWmail/man
/opt/SUNWconn/man
```

- Directory and other management scripts (“`dsserv`” to start/stop the directory server, “`dswebgw`” to start/stop the HTML dirsvc server, etc.):

```
/etc/init.d
```

- Default location of directory configuration files:

```
/etc/opt/SUNWconn/ldap/current
```

- Location of bilk load configuration files:

```
/etc/opt/SUNWmail/dir_svc
```

▼ Saving and Restoring Existing Data in the Directory

Although the directory can’t be used to route mail for SIMS until after it is populated with entries, don’t assume that the current directory is completely empty. Do not use `ldif2ldbm(1M)` or do any other actions which truncate the directory without first saving possible contents using the `ldbmcat(1M)`. Save the contents of the directory for later restoration (using `ldif2ldbm`) as follows:

1. **su to root**

2. **Make sure neither SIMS nor** `dsservd` **are running:**

```
/etc/init.d/im.server stop
/etc/init.d/dsserv stop
```

3. **cd /opt/SUNWconn/sbin**

4. **Decide on a destination directory which has sufficient space to store the contents of the directory in LDIF. In this example we use /tmp.**

5. **Run the `ldbmcat` command.**

   In the C shell:

   ```
   % ./ldbmcat -n /var/opt/SUNWmail/ldap/dbm/id2entry.dbb >&
   /tmp/dbm.ldif
   ```

   Note that if the directory was empty this will produce an empty file. In this case, you do not need to run the subsequent steps to restore data.

6. **After saving the existing data to a file (`/tmp/dbm.ldif` in this example), create the new LDIF for entries you plan to add (ex: `new.ldif`).**

   This process is described in the sections that follow.

7. **Concatenate the new LDIF onto the old.**

   Example: `cat new.ldif >> dbm.ldif`

8. **Load the database with the new LDIF using ldif2ldbm.**

   If your database is not empty then you will have to use the `-c` argument to `ldif2ldbm` to overwrite the database.

   Example: `ldif2ldbm -c -i dbm.ldif`

   Note that faster loading can be attained by using the `-j` parameter to `ldif2ldbm`.

Using `ldif2ldbm` and `ldbmcat` to Initially Populate Local Directories

`ldif2ldbm(1M)` is a way of writing LDIF data directly to the `ldbm` database format used by the directory provided with SIMS. `ldif2ldbm(1M)` must be done locally. It also bypasses certain checks (schema checking of attributes that are mandatory, for example), and therefore may be faster in certain circumstances for bulk-loading large amounts of data into the directory. For example, restoring up a damaged directory from stored LDIF data, or for initially populating a directory from a new batch of LDIF data. Users of `ldif2ldbm` are advised to carefully read the man pages and to practice their proposed use of this tool in an environment where any mistakes will not affect the operation of shared resources. Some important reminders about `ldif2ldbm` are:

- `ldif2ldbm` *truncates* the existing `ldbm` databases when it is invoked, to ensure that no existing data can corrupt the bulk-load it is about to carry out. If you wish to use `ldif2ldbm` on an existing, intact, database, you should use `ldbmcat(1M)`, with ‘`-n`’ flag to first dump the existing `ldbm` database to LDIF, to which the new LDIF is then concatenated, before loading the entire new batch of LDIF data.
- `ldif2ldbm` completely bypasses the directory schema enforced by the `dsservd` directory server. Administrators must be *certain* that data they are entering meets the schema which `dsservd` enforces via it’s `dsserv.conf, dsserv.oc.conf`

and `dsserv.at.conf` files.There are two ways LDIF data may be added to the directory; by using the LDAP protocol (via `ldapmodify(1)`, or by direct modification to the `ldbm` database used by the directory (via `ldif2ldbm(1M)`). Use of the former method is recommended as it does not require you to be on the same system as the database, and automatic merging of existing entries with new values is done. However the latter method may be used by skilled system administrators who are familiar with the procedure, as it requires saving data already in the directory service to prevent data loss.

If you want to verify that your data matches the SIMS schema, use the `imadmin-add-user` utility with your LDIF data to create a few initial users. If you can successfully create users, then the data matches the schema and you can use `ldif2ldbm` to rapidly populate the directory.

Populating the Directory Via the LDAP Server

When you populate the directory, you will perform the following steps:

1. Gather the data used to populate the directory by taking existing data from other naming or directory services (NIS, NIS+, or `/etc/passwd` and `/etc/mail/aliases`)

2. Format the data used to populate the directory to ensure that the data can be read by the `imldifsync(1M)` program

3. Convert the data to LDIF format using the `imldifsync(1M)`command (or your own custom scripts that follow the rules documented below).

Note – imldifsync(1M) replaces ldapsync(1M) (used in earlier versions of the SIMS) for the purposes of generating LDIF for use by SIMS. imldifsync supports the same interfaces as ldapsync, but in addition supports new features such as the client software Web Access. ldapsync is a deprecated interface and will be eliminated in a future release.

---

4. Add/modify LDIF data into the directory database used by the directory service daemon dsserv. Each passwd and alias file entry generates numerous lines of LDIF data based on interpretation rules encoded in imldifsync(1M).

The LDIF attributes and interpretation rules needed by SIMS are listed starting on page 198,. Use these to write your own scripts or translation programs to convert passwd and alias file data into LDIF. We recommend that you use imldifsync(1M)at least as an experimental tool to help you understand how to write scripts that generate LDIF.

Note – After initially populating the directory with NIS/NIS+ user entries, you must also update the directory whenever you update NIS or NIS+ with new email user entries. The procedure we describe for initially populating the directory (in the following sections) is the same procedure for repopulating the directory.

Starting and Stopping SIMS Components

You need to have dsservd running while populating the directory, because imldifsync will communicate with dsserv using LDAP. The IMTA and imaccessd daemon should not be running as they rely on a correctly populated directory to work properly. These programs should be restarted after populating the directory.

To stop imaccessd and all SIMS components use:

```
/etc/init.d/im.server stop
```

When using ldapmodify, ldapadd, or ldapdelete to change what’s in the directory, use the following command to ensure dsservd is running.

```
/etc/init.d/dsserv start
```

Note – The imaccessd process should never be killed using the kill -9 command. Use kill without the -9 argument. If kill -9 is used, run imcheck -c before restarting imaccessd.

Gathering Data Used to Populate the Directory

You will be adding two types of data to the directory:

- user information (from `/etc/passwd` or its equivalent)
- user mail alias and distribution list data from `/etc/mail/aliases` or its equivalent.

This data may come from `/etc` files or from NIS or NIS+ databases. However it must be in a concise format before it can be converted to LDIF by `imldifsync(1M)`

The method for extracting distribution list data depends on whether your system is using NIS, NIS+, or `/etc` files. The following section details how to use the supplied tools to do this for simple user installations. If you have a complex installation you may prefer to write your own tools (using the supplied client side LDAP tools); in that case it is still recommended that you understand the following process before proceeding on your own.

▼ Gathering Directory Data on Systems Using `/etc` Files

The steps below tell how to obtain user-passwd and mail-alias data from system files. When the SIMS IMTA is installed, mail alias and distribution list information is taken from the directory, rather than `/etc/mail/aliases`. Unless you set up a way for `/etc/mail/aliases` to update the directory, it will no longer be used. In this case, you should add a comment in the `/etc/mail/aliases` file to serve as a warning to other system administrators who attempt to add or update aliases.

1. **Log in as root.**

```
$ su
Password: <Enter your root password>
```

Note – During this process be **extremely** careful to not edit `/etc/passwd`!

2. **Change directory to** `/tmp` **and issue the copy command to create a single** `passwd` **file with all the entries required by** `imldifsync(1M)`:

```
# cd /tmp
# sort /etc/passwd > passwd.tmp
# sort /etc/shadow > shadow.tmp
# join -j1 1 -j2 1 -o 1.1 2.2 1.3 1.4 1.5 1.6 1.7 -t: passwd.tmp
shadow.tmp > passwd
# rm passwd.tmp shadow.tmp
```

Note – You may use the passwd and shadow file directly instead of the “join” above by using the “passwd-file” and “shadow-file” options in the `imldifsync.conf` file discussed below.

---

3. **Change directory to** `/tmp` **and issue the copy command as shown to create a mail** `aliases` **file for use by** `imldifsync`:

```
# cd /tmp
# cp /etc/mail/aliases aliases
```

Gathering Directory Data on Systems Using NIS

To obtain user-passwd and mail-alias data from system files, perform the following steps:

1. **Log in as root.**

```
$ su
Password: <Enter your root password>
```

Note – During this process be extremely careful to not edit /etc/passwd!

---

2. **Change directory to** `/tmp` **and issue the** `getent(1M)` **command to create a single** `passwd` **file with all the entries required by** `imldifsync(1M)`:

```
# cd /tmp
# getent passwd > passwd
```

3. **Change directory to** `/tmp` **and issue the** `ypcat(1)` **command as shown to create a mail** `aliases` **file for use by** `imldifsync`:

```
# cd /tmp
# ypcat -k mail.aliases > /tmp/aliases.tmp
# sed ’s/ /: /’ /tmp/aliases.tmp > /tmp/aliases
# rm aliases.tmp
```

▼ Gathering Directory Data on Systems Using NIS+

To obtain user-passwd and mail-alias data from system files, perform the following steps:

1. **Log in as root.**

```
$ su
Password: <Enter your root password>
```

Note – During this process be extremely careful to not edit /etc/passwd!

---

2. **Change directory to** `/tmp` **and issue the** `getent(1M)` **command as shown to create a single passwd file with all the entries required by** `imldifsync(1M)`:

```
# cd /tmp
# getent passwd > passwd
```

3. **Change directory to** `/tmp` **and issue the** `niscat(1)` **command as shown to create a mail** `aliases` **file for use by** `imldifsync`:

```
# cd /tmp
# niscat mail_aliases.org_dir > /tmp/aliases.tmp
# sed ’s/ /: /’ /tmp/aliases.tmp > /tmp/aliases
# rm /tmp/aliases.tmp
```

Formatting Data Used to Populate the Directory

This section describes how to format the user, mail-alias, and distribution list data to successfully populate the directory.

User information must be in the format defined in `passwd(4)`, or as you would find in `/etc/passwd`. An LDIF file will be generated from different fields of each user entry, and user entries will be cross referenced with user alias information (from data you provide of the format found in `aliases(4)`) to create LDIF attribute definitions used by SIMS. The `imldifsync(1M)`command which generates LDIF output makes certain rigid assumptions about the format of the gecos field of a user passwd entry:

`passwd` File Format Rules for `imldifsync(1M)`

The `imldifsync` command converts information in the `passwd` file to LDIF, which is the format required for adding entries to the directory database. If you do not specify your own conversion program or script with the option `—G`, `imldifsync(1M)` uses a default conversion program which expects the gecos field to be in the following format:

```
...:given-name surname, generation-qualifier - comment:...
```

The gecos field is the fifth field in the sequence of colon-separated fields in the `passwd` file.

An example gecos-parsing script which can be used with the -G option is in `/opt/SUNWmail/dir_svc/samples/imgecos2cn.sh`, and may be specified in the `imldifsync.users.conf` or `imldifsync.groups.conf` files (discussed below) via the `gecos2cn-prog` option.

A gecos field that does not conform exactly to this format *may* still be parsed successfully by `imldifsync`, and in this case an LDIF directory entry will be created for it; however, a warning message will be generated for each syntactical error that `imldifsync` encounters, and the resulting attributes may differ from those expected, requiring administrators to make extra efforts to manually ensure the generated LDIF is useful for SIMS.

The following rules are applied when `imldifsync` parses the gecos field:

Rule 1 — General Format

The given-name, surname, and generation-qualifier must start with an alphabetic character, can contain alphabetic characters, dashes (`-`) and single quotes (`’`), and must end with either an alphabetic character or a period (`.`). With the specific exceptions described in “Rule 4 — Surnames” on page 199, uppercase and lowercase characters have no special significance.

The following examples would be converted to valid LDIF directory entries:

- `:Alice Mary White:`
- `:Philip O’Connor, Jr.:`
- `:John-Paul Simon - mktg consultant:`

The following examples would generate a warning message:

- `:+Aaron J. Brown:`
- `:Esther Great!:`
- `:Mary Anderson *sales*:`

Rule 2— Comments

Anything that follows a space-dash-space sequence (-) is interpreted as a comment; also, anything that is enclosed in double quotes or in brackets, even in a non-matching pair, is interpreted as a comment. There can be multiple comments in a single gecos field.

For example:

■ `:Kevin Ascot - Sales Mgr.:`	`the comment is “Sales Mgr.”`
■ `:Brian Scott (surgeon):`	`the comment is “surgeon”`
■ `:Ellen Chelly [CONTRACTOR]:`	`the comment is “CONTRACTOR”`
■ `:Ross "the expert" Brand:`	`the comment is “the expert”`
■ `:Janice Evans (Quality Group}:`	`the comment is “Quality Group”`
■ `:Robert (Bob) Jones - Mktg:`	`the comments are “Bob” and “Mktg”`

Rule 3— Generation-Qualifiers

If there is a comma anywhere in the gecos field (except in comments), the words that follow it are interpreted as a generation-qualifier. The generation-qualifier is optional, but if present, it must not be blank.

The following examples would be converted to valid LDIF directory entries:

- `:John Smith,Jr.:`
- `:John Smith, Senior:`

The following examples would generate a warning message:

- `:John Smith,:`
- `:John Smith, - Snr:`

Rule 4 — Surnames

The surname is either the last word in the gecos field, or the last word before either a generation-qualifier or a comment. If there is only one word in the gecos field, it is assumed to be the surname. If there are no words in the gecos field, the username is assumed to be the surname.

For example:

■ `:Kate Black:`	the surname is “black”
■ `:Ann Mary Wells:`	the surname is “Wells”

`:John Smith, Jr.:`	the surname is “Smith”
`:Erwin David BLINK - Engineer:`	the surname is “BLINK”

Surnames can also consist of several words. In this case, the capitalization is used to distinguish between words that are part of the given-name and words that are part of the surname.

Words that immediately precede the surname, and that are also either *all uppercase* or *all lowercase* are interpreted to be part of the surname. This allows naming prepositions such as “le” or “de” in french, and “von” or “van” in german, to be interpreted correctly.

For example:

`:Jean-Pierre le GAD:`	the surname is “le GAD”
`:Joe van der Graf:`	the surname is “van der Graf”
`:Jose MARCOS SOUZA:`	the surname is “MARCOS SOUZA”
`:Franz Josef von Bismark:`	the surname is “von Bismark”

Note the unexpected effect that the application of this rule may have if the gecos field is all lowercase or all uppercase, or if there is an initial letter preceding the surname.

For example:

`:gerhard ellis sumner:`	the surname is “gerhard ellis sumner”
`:ADRIENNE CHIU (sales):`	the surname is “ADRIENNE CHIU”
`:Peter K. Wolff:`	the surname is “K. Wolff”

Rule 5 — Given-Name

Once the other components of the gecos field have been identified, the remaining words are interpreted as the given-name.

For example:

`:Jean-Pierre le GAD:`	the surname is “gerhard ellis sumner”
`:Joe van der Graf:`	the given-name is “Joe”
`:Jose MARCOS SOUZA:`	the given-name is “Jose”
`:Franz Josef von Bismark:`	the given-name is “Franz Josef”
`:Peter K. Wolff:`	the given-name is “Peter”

If your user passwd information does not meet this criteria then you have three alternatives:

- Convert the passwd data to the above format required by `imldifsync(1M)`, using your own custom written scripts to modify the gecos field. Run `imldifsync` using that data.
- Write your own gecos parsing script as documented in the `imldifsync` manpage, using the example `gcos2cn.sh`, in `/opt/SUNWmail/ldap/samples`, and pass that to `imldifsync(1M)` via the `-G` flag
- Do not use `imldifsync` at all, but instead write your own LDIF generator that produces LDIF entries with the attributes that SIMS requires.

▼ `aliases` File Format for `imldifsync`

The `imldifsync`(1M) command makes assumptions about the format of the mail `aliases` file used as input. The command uses the information in the `aliases` file to generate attributes for an entry. The expected format for the `aliases` file is described below.

Note – Refer to the manpage for the `aliases(4)` file for general usage information.

Rule 1 — General Format for User Aliases

For each user, the `aliases` file must contain two lines in the following format:

```
userid: first.lastname
first.lastname: userid@mailhost
```

where:

userid is the same as the user ID in the first field of the `passwd` file

first.lastname is usually a concatenation of the user’s given name and surname

mailhost is the machine where the user’s mailbox resides.

When the `aliases` file contains this type of information for a user, `imldifsync(1M)` creates the following attributes:

- `rfc822MailAlias` with value *first.lastname@maildomain*
- `mail` with values *first.lastname@mailhost.maildomain*, *userid@mailhost.maildomain*, and also with the same value as `rfc822MailAlias`
- `mailDeliveryOption` with value *mailbox*
- `mailHost` with value *mailhost.maildomain*

- `ispAuthorizedServices` with values *imap, imaps, pop3, sunw_webaccess, sunw_calendar*
- `inetUserMailVersion` with value *1.0*
- `inetSubscriberStatus` with value *active*

Note – The *maildomain* in the attribute values is the mail domain declared in the configuration file for the `imldifsync` command. This mail domain must be the same as the one declared in the `dsserv.conf` configuration file.

For example, the `aliases` file contains the following lines for user Allyn Robinson:

```
arobin: allyn.robinson
allyn.robinson:arobin@cloud
```

The `imldifsync` command extracts the following attributes and attribute values from this information:

```
rfc822MailAlias: allyn.robinson@Marketing.stream.com
mail: allyn.robinson@cloud.Marketing.stream.com
mail: arobin@cloud.Marketing.stream.com
mail: allyn.robinson@Marketing.stream.com
mailDeliveryOption: mailbox
mailHost: cloud.Marketing.stream.com
ispAuthorizedServices: imap
ispAuthorizedServices: imaps
ispAuthorizedServices: pop3
ispAuthorizedServices: sunw_webaccess
ispAuthorizedServices: sunw_calendar
inetUserMailVersion: 1.0
inetSubscriberStatus: active
```

Rule 2 — Handling Differing User IDs

The user ID supplied on the first line can be different from the user ID on the second line.

```
userid1: first.lastname
first.lastname: userid2@mailhost
```

In such cases, `imldifsync(1M)` creates the `mailDeliveryOption` attribute with the value **forward**, and also creates a `mailForwardingAddress` attribute.

For example, the `aliases` file could contain the following lines for user Allyn Robinson:

```
arobin: allyn.robinson
allyn.robinson:jconnors@cloud
```

The `imldifsync` command extracts the following attributes and attribute values from this information:

```
rfc822MailAlias: allyn.robinson@Marketing.stream.com
mailForwardingAddress: allyn.robinson@cloud.Marketing.stream.com
mailForwardingAddress: jconnors@cloud.Marketing.stream.com
mailDeliveryOption: forward
```

Combining Rule 1 and Rule 2

You can combine the general format described in Rule 1 with the format described in Rule 2, as follows:

```
userid1: first.lastname
first.lastname: userid1@mailbox, userid2@mailhost
```

In such cases, `imldifsync(1M)`creates the `mailDeliveryOption` attribute with the values **mailbox** and **forward**, and creates the `mailForwardingAddress` attribute.

For example, the `aliases` file could contain the following lines for user Allyn Robinson:

```
arobin: allyn.robinson
allyn.robinson:arobin@cloud, jconnors@cloud
```

The imldifsync command extracts the following attributes and attribute values from this information:

```
rfc822MailAlias: allyn.robinson@Marketing.stream.com
mail: allyn.robinson@cloud.Marketing.stream.com
mail: arobin@cloud.Marketing.stream.com
mail: allyn.robinson@Marketing.stream.com
mailForwardingAddress: jconnors@cloud.Marketing.stream.com
mailDeliveryOption: mailbox
mailDeliveryOption: forward
mailHost: cloud.Marketing.stream.com
```

Rule 3— Handling Nicknames

An aliases file can contain more than two lines per user, in which case, the format to observe is:

```
userid: first.lastname
nickname1:first.lastname
nickname2:first.lastname
first.lastname: userid@mailhost
```

In such cases, the imldifsync(1M) command creates the rfc822Mailbox attribute with an extra value for each nickname.

For example, the aliases file could contain the following lines for user Allyn Robinson:

```
arobin: allyn.robinson
arobinson: allyn.robinson
allyn: allyn.robinson
allyn.robinson: arobin@cloud
```

The imldifsync command extracts the following attributes and attribute values from this information:

```
rfc822MailAlias: allyn.robinson@Marketing.stream.com
mail: allyn.robinson@Marketing.stream.com
mailDeliveryOption: mailbox
mailHost: cloud.Marketing.stream.com
```

Rule 4— Handling File Names in Aliases

A user alias in the `aliases` file can contain a file name, following this format:

```
userid: first.lastname
first.lastname: filename
```

where *filename* must start with a slash (/).

In such cases, `imldifsync(1M)` creates the `mailDeliveryOption` attribute with the value “file”, and also creates a `mailDeliveryFile` attribute.

For example, the `aliases` file could contain the following lines for user Allyn Robinson:

```
arobin: allyn.robinson
allyn.robinson:/var/allyn/mail
```

The `imldifsync` command extracts the following attributes and attribute values from this information:

```
rfc822MailAlias: allyn.robinson@Marketing.stream.com
mailForwardingAddress: allyn.robinson@cloud.Marketing.stream.com
mailDeliveryFile: /var/allyn/mail
mailDeliveryOption: forward
mailDeliveryOption: file
```

Rule 5— Handling Program Names in Aliases

A user alias in the `aliases` file can contain a program name, following this format:

```
userid: first.lastname
first.lastname: |programName
```

Note that the pipe (|) symbol is required to introduce a program name.

In such cases, `imldifsync(1M)`creates the `mailDeliveryOption` attribute with the value “program”, and also creates a `mailProgramDeliveryInfo` attribute.

For example, the `aliases` file could contain the following lines for user Allyn Robinson:

```
arobin: allyn.robinson
allyn.robinson:|/bin/cat
```

The `imldifsync` command extracts the following attributes and attribute values from this information:

```
rfc822MailAlias: allyn.robinson@Marketing.stream.com
mailForwardingAddress: allyn.robinson@cloud.Marketing.stream.com
mailProgramDeliveryInfo:  /bin/cat
mailDeliveryOption: forward
mailDeliveryOption: program
```

Rule 6— General Format for Group Aliases

For each group (distribution list), the `aliases` file must contain two lines in the following format:

```
owner-aliasname: owner1 [owner2 ...]
[aliasname-request: processor]
aliasname: user1, user2, user3 ...
```

where:

aliasname is the name of the alias

owner1, *owner2*, ... are the names of the owners of the alias. An owner can be a member of the group, but not necessarily.

processor is the name of entity who will be responsible for processing requests sent to the alias

user1, user2, user3, ... are the members of the alias

The owner, processor and member entities defined above can be:

- A person with an entry in the directory
- A person known by an rfc822 mail address without an entry in the directory
- A program, introduced by the pipe (|) symbol
- A file, introduced by a slash (/)

Depending on where you obtained your data (`/etc` files, NIS, NIS+) you may have to further format data.

Converting the Data to LDIF Format

LDIF (LDAP Data Interchange Format) is a canonical data form used to represent entries in LDAP databases. Currently a draft-Internet-RFC, LDIF is designed to be a transportable intermediate data form that is portable between LDAP directories. Data must be converted to LDIF before it can be added to the directory. Administrators may use one of several methods to generate LDIF:

- Use the supplied `imldifsync(1M)` program to synchronize input data with data already added to the directory (if such exists).
- Write your own scripts or programs to generate LDIF based on `passwd`, user alias, and distribution list data.

Note – Although this section will involve two files; `passwd` data first, `alias`/distribution-list data second, both user passwd and user alias information will be required in the first pass. Do not continue until you have both data-sets ready to use.

A Few Words About `imldifsync(1M)`

`imldifsync(1M)` does several things:

- maps password and alias entry information into LDIF output.
- correlates password file user entries with alias file user entries.
- creates certain LDIF attribute values based on `passwd` and `alias` input.
- fabricates certain DNs required by `dsservd` if they are not present in the ldbm.
- synchronizes changes in the input password and alias files and converts those differences to LDIF. `imldifsync` may be used to periodically synchronize the LDAP directory with changes to the password and alias files (for example, if users are added or deleted to the password or alias file).

The default configuration files, `imldifsync.users.conf` and `imldifsync.groups.conf`, are installed in `/etc/opt/SUNWmail/dir_svc/`. Converting data using `imldifsync` is a two phase process. First, the user/passwd data is converted, then the mail-alias/groups data. The two default configuration files are required, one for each phase.

The SIMS installation GUI will set certain values in the default `imldifsync.users.conf` and `imldifsync.groups.conf` based on your input. You should keep track of the settings by keeping an untouched copy of these files.

Note – The `imldifsync.users.conf` and `imldifsync.groups.conf` files are readable only by `root`, because the file contains the “bind-DN” and “ldap-passwd” directives, which the SIMS install GUI will set based on what you enter as your Administrative password. You should be aware that anyone with this bind-DN and password can change any aspect of the Directory contents or configuration, and guard the bind-DN and password appropriately.

Converting the Data to LDIF Format Using `imldifsync(1M)`, and Adding Data to the Directory Using `ldapmodify(1M)`.

1. **Change directories to and make a copy of the** `imldifsync.users.conf` **and** `imldifsync.groups.conf` **files as configured by the SIMS install process.**

   In the event the modified versions of the `imldifsync.users.conf` and `imldifsync.groups.conf` files are lost or damaged you will have the original file saved.

```
# cd /etc/opt/SUNWmail/dir_svc
# cp imldifsync.conf imldifsync.conf.SIMS3.5
# vi imldifsync.conf
```

2. **Edit the** `imldifsync.users.conf` **and** `imldifsync.groups.conf` **file.**

   Uncomment the `passwd-file`, and `aliases-file` files, and change their values as shown:

```
passwd-file = "/tmp/passwd"
aliases-file = "/tmp/aliases"
```

By default the `imldifsync.users.conf` file contains two lines like this:

```
add-val = { "mailFolderMap: SUN-MS" }
ignore-attr = { "mailFolderMap" }
```

“SUN-MS” is the recommended mailstore for SIMS. However if you chose to use the “/var/mail” type of message store during your Install, you should change “SUN-MS” to “UNIX V7”.

You may choose to add other attributes here as well, but there are two rules that must be followed:

- Only attributes from the default SIMS schema may be added in this way. User created attributes cannot be added through this interface.
- As shown in the example, only attributes which have values common to all users (for the user data generation pass) or groups (for the group/alias-data generation pass) should be added here.

3. **If you want to set a user mail store quota edit `users.conf`.**

   The SIMS default setting is "no limit." To set a space limit, modify the `mailQuota` attribute as follows:

```
add-val = { “mailQuota: <quota in bytes>” , “mailFolderMap: SUN-MS” }
```

   where `<quota in bytes>` would be 10000000 if you wanted to set a mail space quota of 10 megabytes. See "Message Store Quotas" on page 162 for detailed information on setting quotas.

4. **Convert the user data to LDIF format.**

   Use the `imldifsync` command to generate formatted user data (`LDIF`) by issuing the following command:

```
# /opt/SUNWmail/sbin/imldifsync -c imldifsync.users.conf > /tmp/
imldifsync.users.ldif
```

5. **Populate the directory with the user LDIF formatted data.**

   This must be done before running imldifsync during the alias-data generation pass because imldifsync compares existing data in the directory to newly generated data to determine what will be generated as the groups data.

   Use the `ldapmodify` command to add the new entries to the directory:

```
# /opt/SUNWmail/bin/ldapmodify -D bind-DN -w ldap-passwd -f /tmp/
users.ldif
```

   Refer to the bulleted section above for `bind-DN` and `ldap-password` information.

Note – If you already have some entries in the Directory database you should specify the -c argument to ldapmodify in addition to those above, so that ldapmodify will continue to the new entries. `ldapmodify` will otherwise exit if it tries to add an entry that is already in the Directory.

---

6. **Convert the aliases/distribution-list data to LDIF format.**

   Use the `imldifsync` command to generate formatted user data (LDIF) by issuing the following command:

```
# /opt/SUNWmail/sbin/imldifsync -c imldifsync.groups.conf > /tmp/
groups.ldif
```

7. **Populate the directory with the aliases/distribution-list LDIF formatted data.**

   Use the `ldapmodify` command to add the new entries to the directory:

```
# /opt/SUNWmail/bin/ldapmodify -D bind-DN -w ldap-passwd -f /tmp/
groups.ldif
```

Refer to the bulleted section above for `bind-DN` and `ldap-password` information.

Note – If you already have some entries in the Directory database you should specify the `-c` argument to `ldapmodify` in addition to those above, so that ldapmodify will continue to the new entries. ldapmodify will otherwise exit if it tries to add an entry that is already in the Directory.

LDAP Data Interchange Format

The LDAP Data Interchange Format (LDIF) is used to represent LDAP entries in text form. The `ldif2ldbm`(1M) tools can be used to convert from LDIF format to the LDBM format used by `slapd(8)`. The `ldbmcat(1M)` tool can be used to do the reverse conversion.

The basic form of an LDIF entry is:

```
[id]
dn: distinguished name
attrtype: attrvalue
attrtype: attrvalue
...
```

where *id* is the optional entry ID (a positive decimal number). By default, the database creation tools supply the ID for you. The `ldbmcat(1M)` program, however, produces an LDIF format that includes *id* so that new indexes created are consistent with the existing database. A line may be continued by starting the next line with a single space character, for example,

```
cn: Anne Yoshikawa
 Jones
```

Multiple attribute values are specified on separate lines, for example,

```
cn: Ann Jones
cn: Annie Jones
```

If an *attrvalue* contains a non-printing character, or begins with a space or a colon (:), the *attrtyp* is followed by a double colon and the value is encoded in base 64 notation. For example, the value "begins with a space" would be encoded like this:

```
cn:: IGJlZ2lucyB3aXRoIGEgc3BhY2U=
```

Multiple entries within the same LDIF file are separated by blank lines.

LDIF Examples

For more examples refer to the *SIMS Provisioning Guide*.

CODE EXAMPLE 9-1 LDAP file with two entries

```
dn: cn=Barbara Jensen,ou=People,dc=stream,dc=com,o=internet
objectclass: top
objectclass: person
objectclass: organizationalPerson
cn: Barbara Jensen
cn: Barbara J Jensen
cn: Babs Jensen
sn: Jensen
uid: bjensen
telephonenumber: +1 408 555 1212
description: A big sailing fan.

dn: cn=Bjorn Jensen,ou=People,dc=stream,dc=com,o=internet
objectclass: top
objectclass: person
```

CODE EXAMPLE 9-1 LDAP file with two entries

```
objectclass: organizationalPerson
cn: Bjorn Jensen
sn: Jensen
telephonenumber: +1 408 555 1212
```

CODE EXAMPLE 9-2 LDAP File Containing a Base-64-encoded Value

```
dn: cn=Gern Jensen,ou=People,dc=stream,dc=com,o=internet
objectclass: top
objectclass: person
objectclass: organizationalPerson
cn: Gern Jensen
cn: Gern O Jensen
sn: Jensen
uid: gernj
telephonenumber: +1 408 555 1212
description::
V2hhdCBhIGNhcmVmdWwgcmVhZGVyIHlvdSBhcmUhICBUaGlzIHZhbHVlIGlzIGJ
hc2UtNjQtZW5jb2RlZCBiZWNhdXNlIGl0IGhhcyBhIGNvbnRyb2wgY2hhcmFjdGV
yIGluIGl0IChhIENSKS4NICBCeSB0aGUgd2F5LCB5b3Ugc2hvdWxkIHJlYWxseSB
nZXQgb3V0IG1vcmUu
```

CODE EXAMPLE 9-3 LDAP File Containing a Reference to an External File

```
dn: cn=Horatio Jensen,ou=People,dc=stream,dc=com,o=internet
objectclass: top
objectclass: person
objectclass: organizationalPerson
cn: Horatio Jensen
cn: Horatio N Jensen
sn: Jensen
uid: hjensen
telephonenumber: +1 408 555 1212
jpegphoto:< file:///usr/local/directory/photos/hjensen.jpg
```

CODE EXAMPLE 9-4 LDAP File Containing a Value in non-UTF-8 Encoding

```
dn: cn=Rolf Sorensen,ou=People,dc=stream,dc=com,o=internet
objectclass: top
objectclass: person
objectclass: organizationalPerson
cn: Rolf Sorensen
cn;charset=ISO-8859-1:: Um9sZiBT+HJlbnNlbg==
sn: Sorensen
sn;charset=ISO-8859-1:: U/hyZW5zZW4K
uid: rsor
telephonenumber: +1 408 555 1212
```

CHAPTER 10

Secure Sockets Layer (SSL) Support in SIMS

SSL Overview

The Secure Sockets Layer (SSL) is an open, non-proprietary security protocol. It has been submitted to the W3 Consortium (W3C) Working Group on Security for consideration as a standard security approach for World-Wide Web browsers and servers on the Internet. SSL provides data encryption, server authentication, message integrity, and optional client authentication for a TCP/IP connection.

Using SSL with SIMS ensures security between a mail client and SIMS by encrypting email content sent by the SIMS server to the email client.

Authentication by Certificate

A certificate is a nontransferable digital file that contains certain identifying, information. Specifically, a certificate contains the issuer’s identity, the receiver’s identity, and the public key. The certificate is issued from a third-party whom both parties trust. This third party is known as a Certificate Authority (CA).

A Certificate Authority (CA) can be *internal*—you create certificates within your organization, or *external*— a third party can issue a certificate for you.

Both servers and clients can have certificates. When a server sends a certificate to a client, the process is called *server authentication*. When a client sends a certificate to a server the process is called *client authentication*. If you plan on using SSL on your server, you must obtain a server certificate from a valid CA.

Note – At the present time, SIMS only supports server authentication via SSL.

Secure Public-Key Management Infrastructure (SKI) Overview

If you are already familiar with SKI, you may wish to skip to "SSL Installation" on page 218 and begin installation.

Solaris Server products that provide SSL service typically use a system called SKI as the means of implementing basic Public-Key Infrastructure (PKI) functionality, for example, key and certificate storage and management. The SKI tools permit the user to create and manage key packages (a cryptographically protected container for an entity's public and private keys), and to create and/or manage X.509 certificates. The following sections present a brief overview of those portions of SKI that will be used to administer server certificates. More information can be found in the SKI man pages whose default installation path is `/opt/SUNWski/man`.

The **`skiserv`** Daemon

While not a command that administrators will typically deal with directly, the SKI server, `skiserv`, is worth mentioning. The SKI server is responsible for providing a server process appropriate access to the key packages that it needs to complete a particular SSL connection. The SKI server will provide to the requesting process access to key packages on the basis of process UID and the IP address upon which the SSL connection is being accepted. In order to gain access to any given key package's private key, the SKI server must be provided with a password to unlock the key package. For server key packages, this is typically done with the `skilogin -h` command. If the administrator wishes to start or stop the SKI server, she may do so with the following commands:

```
# su root
# /etc/init.d/skiserv stop
```

and

```
# /etc/init.d/skiserv start
```

The **keypkg** Command

The `keypkg` command is used to create and administer a server's key package(s). A server's key package must be created prior to issuing a Certificate Signing Request (CSR).

The **skilogin -h** Command

The `skilogin -h` command effectively binds a key package to a UID and IP address. That is, when a server process requests a key package, it will be provided on the basis of that process's UID and the IP address upon which an incoming SSL connection is being accepted. When issuing the `skilogin` command, the administrator must provide the password which will unlock the key package's private key. The `skilogin -h` command must be issued for each UID and IP binding that the administrator wishes to create.

The **skilogout -h** Command

The `skilogout -h` command revokes the SKI server's access to a key package. That is, it removes the binding that exists between the key package, UID, and IP address.

The **skicert** Command

The `skicert` command allows the administrator to view and remove X.509 certificates stored in the SKI repository. Certificates are stored into the repository using the `skistore` command. The `skicert -S` command is also useful for examining certificates stored in files, for example, a certificate received from a CA.

The **certreq -h** Command

The `certreq -h` command allows the administrator to issue a Certificate Signing Request (CSR) for a server key package associated with a specific UID and IP address binding. Submission of a CSR to a CA will produce an X.509 certificate.

The `skistore` Command

The `skistore` command can be used to store an X.509 certificate into the SKI repository. Use of this command is typically the final step in the setup and installation of a server certificate.

SSL Installation

STOP! Before actually performing the instructions described here, it is very important that you familiarize yourself with all the steps described in this section. It will also help if you review the “SSL Examples” on page 224 before attempting the actual SSL configuration. This section provides the template for the operations you will need to configure SSL for SIMS.

Before a server can use SSL, it must have public and private keys which are used for server authentication, and an X.509 certificate that vouches for its identity. The certificate contains the server’s identity (in the form of an X.500 distinguished name, or DN), the server’s public key, and the digital signature of the certificate authority, or CA, that issued the certificate. Generally speaking, the administrator of a service secured by SSL will need to accomplish the following steps:

1. “Choose an Appropriate Certificate Authority (CA)” on page 219.

2. “Create the Server Key Package and Register it with SKI Key Server” on page 220.

3. “Create the Certificate Signing Request” on page 221

4. “Submit the Certificate Signing Request to the Chosen CA” on page 221.

5. “Install the Server Certificate Produced by the CA” on page 222.

6. “Install the Root CA Certificate Provided by the CA” on page 222.

These instructions will guide an administrator through the steps necessary to produce and install a server certificate, signed by either a CA created by the administrator or by a commercial CA, such as VeriSign.

▼ Choose an Appropriate Certificate Authority (CA)

If a commercial certificate vendor is to be used, for example VeriSign, then skip to "Create the Server Key Package and Register it with SKI Key Server" on page 220. Otherwise, you will need to create an internal root certificate authority (CA) using the following instructions.

▼ Create the UNIX Account for the Internal Root CA

Create a UNIX account for the user who will act as the Root CA. Standard practice is to locate the Root CA on a machine disconnected from the network and located in a secure area. If you configure a machine in this fashion, you will have to develop a secure methodology for information transfer. An example of this would be Certificate Signing Requests and certificates between the Root CA machine and the server machine. For testing purposes, you may wish to collocate the Root CA with the server, but be aware that this may place the integrity of the Root CA at risk.

For the purposes of these instructions, we shall select `skirca` as the UNIX user name of the Root CA. If you have not already done so, create a UNIX user with user id of skirca on your system used to create the Root CA.

▼ Create the Internal Root CA Credentials

Issue the following command:

```
*** On the Root CA machine:
# su skirca
# /usr/bin/crca
```

Respond to the queries presented as follows:

1. **Distinguished Name:**

   Can be any X.500 distinguished name, but we suggest at minimum that the `CN`, `O`, and `C` attributes be specified, for example:

   CN=SUPERDUPERCA, O=OURCO, C=US

2. Directory for Storing Root CA Credentials:

   Specify the full pathname of the directory into which will be stored a copy of the Root CA credentials, for example:

   /export/home/skirca/ca-creds

Strictly speaking, once the `crca` command has completed, you could delete this directory, as all pertinent information has been stored in the SKI repository. Leaving this directory intact may help in the future should the SKI repository become corrupted. It is also useful should it become necessary to store the Root CA certificate on a machine other than the Root CA machine.

3. **`Do you want to store Root CA creds in the naming service[y/n]:`**

   Enter **y**.

4. Finally, you will be queried for the root user password. This will permit the `crca` command to store the Root CA credentials into the SKI repository.

▼ Create the Server Key Package and Register it with SKI Key Server

Log into the server machine to be secured and issue the following commands:

```
*** On the server machine:
```

```
# su root
# keypkg -Ch
# skilogin -h 0
# skilogin -h <server-uid-number>
```

You will be queried for the server/host DN. This DN should be formed in the following fashion:

```
CN=<common-name>,OU=<org-unit>,O=<org>,ST=<full-state-or-provinc
e-name>,C=<iso-country-code>
```

For example:

```
CN=OURCOSERVER, OU=SALES, O=OURCO, ST=CALIFORNIA, C=US
```

Be sure to specify all of the above listed attributes, in the order specified, as certain commercial certificate vendors, for example, Verisign, require the server DN be specified in this fashion.

The two invocations of the `skilogin` command will grant access to processes running with the specified UIDs. You will be queried for the password that will unlock the server key package. This is the same password that was used to lock the key package when it was created using the `keypkg` command. Do not lose this password or future administrative procedures may require the creation of a new server key package and certificate.

`<server-uid-number>` can be determined with the following command:

```
# id <server-uid-name>
```

where <server-uid-name> is the UNIX user name as which the server process is run.

Note: The SIMS message access server imaccessd by default runs as user inetmail, so for the key package to be used by this service, you would determine <server-uid-number> using the following command:

```
# id inetmail
```

Using SSL in a Multiple IP Address Environment

If SSL is to be used in a Multiple IP Address environment, you will need to bind the key package to multiple IP addresses. For each IP address to which you wish to bind the key package, you will need to issue a command of the form:

```
*** On the server machine:
```

```
# skilogin -h -L <ip-address> <server-uid-number>
```

▼ Create the Certificate Signing Request

Once a suitable server key package is available, you should then generate a Certificate Signing Request using the following command sequence:

```
*** On the server machine:
```

```
# su root
# certreq -bh <csr-file>
```

Where <csr-file> is the pathname to a file into which will be written the Certificate Signing Request.

▼ Submit the Certificate Signing Request to the Chosen CA

If you are using a commercial certificate vendor, present the contents of <csr-file> to the CA using the instructions provided by the certificate vendor, and then proceed to “Install the Server Certificate Produced by the CA” on page 222.

If you are using an internal root CA, as was described in “Create the Internal Root CA Credentials” on page 219, transfer the <csr-file> to the Root CA machine using whatever means are appropriate, and proceed with the following instructions:

```
*** On the Root CA machine:
```

```
# su skirca
# skilogin
# certify -o <server-cert-file> <csr-file>
# skilogout
```

where <**server-cert-file**> is a pathname to a file that will receive the new certificate.

▼ Install the Server Certificate Produced by the CA

Assuming that you have received or produced a new certificate and have transferred its contents to the server machine, in a file we'll identify as <server-cert-file>, proceed with the following instructions:

```
*** On the server machine:
```

```
# su root
# skistore -c <server-cert-file> -k <server-dn>
```

where <server-dn> is the DN from the key package that was created in "Create the Server Key Package and Register it with SKI Key Server" on page 220. For example:

```
# skistore -c ourco.cert -k \
'CN=OURCOSERVER, OU=SALES, O=OURCO, ST=CALIFORNIA, C=US'
```

▼ Install the Root CA Certificate Provided by the CA

For SSL server security to function properly, you must install the Root CA certificate of the CA that produced your server certificate. In the general case, this is accomplished in the following fashion:

```
*** On the server machine:
```

```
# su root
# skistore -c <rootca-cert-file> -k <rootca-dn>
# keypkg -Ah <rootca-cert-file>
```

where <rootca-cert-file> contains the certificate of the Root CA that created the server certificate and <rootca-dn> specifies the Root CA's DN. The <rootca-cert-file> file must be obtained by whatever means are provided by the commercial certificate vendor. Once you have obtained the Root CA certificate, you may determine the DN of the Root CA using the following command:

```
# skicert -S <rootca-cert-file> | egrep "Issuer" | \
awk -F\: ’print {$2}’
```

If you have implemented an internal Root CA, you may log into the Root CA machine as the Root CA user, for example `skirca`, and obtain the Root CA certificate in the following manner:

```
*** On the Root CA machine:
```

```
# su skirca
# skicert -F -k <rootca-dn> <rootca-cert-file>
```

for example:

```
# skicert -F -k ’CN=SUPERDUPERCA, O=OURCO, C=US’ superduperca.cert
```

You may then transfer the `<rootca-cert-file>` to the server machine and install using the `skistore/keypkg` command sequence specified above.

Note – The SWS 2.1 packages included with SIMS 4.0, install copies of the most common Verisign Root CA certificates in the following directory:

```
/usr/http/certs
```

You may use the appropriate `<root-ca-file>` if your server certificate was produced by Verisign Inc.

After determining the DN of a Verisign Root CA certificate, note that the DN contains a comma in the `O=...` attribute. Depending upon the command line shell in use by the site administrator, special care must be taken to insure that the DN is correctly specified when using skistore command, for example,

```
# su root
#skistore -c VerisignCA.cert -k \
    ’OU=SECURE SERVER CERTIFICATION AUTHORITY, O=RSA DATA SECURITY,
INC., C=US’
# keypkg -Ah VerisignCA.cert
```

Enable SSL Operation

The SIMS product ships with SSL enabled by default. Once the server credentials are properly installed, no additional administrative steps are necessary.

SSL Examples

Example of Creation of Self-signed Server Certificate

The following is an example of the steps taken to create a server certificate using an internal local Root CA. This example assumes the following:

- The user “skirca” has been created as the Root CA UNIX user.
- The “skirca” home directory is: `/export/home/skirca`
- The Root CA is co-located on the machine on which the server certificate will be installed. This simplifies the example but should not be considered secure.

1. **First, create the Root CA credentials...**

```
% su skirca
% /usr/bin/crca
#
# Distinguished Name:
#

Enter Distinguished Name (e.g. "o=SUN, c=US")
or q[uit]: CN=SUPERDUPERCA, O=OURCO, C=US


#
# Directory for Storing RootCA Credentials:
#

Enter directory pathname under which the key package and
certificate will be stored, or q[uit].
Directory name ? /export/home/skirca/rootca-creds


keypkg: Generating RSA key pair for user "CN=SUPERDUPERCA,
O=OURCO, C=US"

\
keypkg: Enter your NEW key package password:
<enter root ca key package password>
keypkg: Reenter your NEW key package password:
<enter root ca key package password>
keypkg: Key package generation succeeded
certify: Certificates issued:6, certificates available:4
#
#  Do you want to store RootCA creds in the naming service
[y/n]: y

#
# Storing the RootCA creds in the naming service
# You need to enter the root password
Password:
<enter root UNIX user password>
skistore: keypkg
/export/home/skirca/rootca-creds/keypkgs/skirca.KEYPKG
successfully stored
skistore: certificate
/export/home/skirca/rootca-creds/certs/skirca.CERT successfully
stored
skistore: Operation Completed

#
# The Rootca creds are stored in the naming service
```

2. **Next, create the server key package...**

```
% su root
% /usr/bin/keypkg -Ch
/usr/bin/keypkg: Enter Distinguished Name of key package owner,
or ’q’ for ’quit’: CN=OURCOSERVER, OU=SALES, O=OURCO,
ST=CALIFORNIA, C=US
/usr/bin/keypkg: Generating RSA key pair for user
"CN=OURCOSERVER, OU=SALES, O=OURCO, ST=CALIFORNIA, C=US"

/usr/bin/keypkg: Enter your NEW key package password:
<enter host key package password>
/usr/bin/keypkg: Reenter your NEW key package password:
<enter host key package password>
/usr/bin/keypkg: Key package generation succeeded

% /usr/bin/skilogin -h 0
/usr/bin/skilogin: Enter host key package password:
<enter host key package password>

% id inetmail
```

```
uid=72(inetmail) gid=6(mail)

% /usr/bin/skilogin -h 72
/usr/bin/skilogin: Enter host key package password:
<enter host key package password>
```

3. **Next, create the certificate signing request (CSR)...**

```
% /usr/bin/certreq -bh /export/home/skirca/ourcoserver.csr

% chmod a+r /export/home/skirca/ourcoserver.csr
```

4. **Next, submit the CSR to the internal root CA...**

```
% su skirca

% /usr/bin/skilogin
/usr/bin/skilogin: Enter your own key package password:
<enter root ca key package password>

% /usr/bin/certify -o /export/home/skirca/ourcoserver.cert
/export/home/skirca/ourcoserver.csr
/usr/bin/certify: Certificates issued:7, certificates
available:3

% /usr/bin/skilogout
```

5. **Next, install the server certificate produced by the internal root CA...**

```
% su root

% /usr/bin/skistore -c /export/home/skirca/ourcoserver.cert -k
'CN=OURCOSERVER, OU=SALES, O=OURCO, ST=CALIFORNIA, C=US'
/usr/bin/skistore: certificate
/export/home/skirca/ourcoserver.cert successfully stored
/usr/bin/skistore: Operation Completed
```

It should now be possible to make connections to the SSL-enabled IMAP and POP ports.

Example of Creation of Externally Signed Server Certificate:

The following is an example of the steps taken to create a server certificate using an external Root CA. Verisign Inc. is the Root CA used in this example. This example assumes the following:

- A working directory is available. In this example, we'll call it: `/export/home/inetmail`

1. **First, create the server key package...**

```
% su root

% /usr/bin/keypkg -Ch
/usr/bin/keypkg: Enter Distinguished Name of key package owner,
or ’q’ for ’quit’: CN=OURCOSERVER, OU=SALES, O=OURCO,
ST=CALIFORNIA, C=US
/usr/bin/keypkg: Generating RSA key pair for user
"CN=OURCOSERVER, OU=SALES, O=OURCO, ST=CALIFORNIA, C=US"

/usr/bin/keypkg: Enter your NEW key package password:
<enter host key package password>
/usr/bin/keypkg: Reenter your NEW key package password:
<enter host key package password>
/usr/bin/keypkg: Key package generation succeeded

% /usr/bin/skilogin -h 0
/usr/bin/skilogin: Enter host key package password:
<enter host key package password>

% id inetmail
uid=72(inetmail) gid=6(mail)

% /usr/bin/skilogin -h 72
/usr/bin/skilogin: Enter host key package password:
<enter host key package password>
```

2. **Next, create the certificate signing request (CSR)...**

```
% /usr/bin/certreq -bh /export/home/inetmail/ourcoserver.csr
```

3. **Next, submit the CSR to the external Root CA, in this case, Verisign Inc.**

The CSR is in the file `/export/home/inetmail/ourcoserver.csr`, and should be submitted to Verisign using the instructions that are provided by the Verisign web site.

4. **Next, install the server certificate produced by the external Root CA.**

Verisign will email the new server certificate to the email address provided when you submitted the CSR. The message should contain a block of data that looks something like:

```
-----BEGIN CERTIFICATE-----
MIIB3DCCAUUCBgUqk4+ncTANBgkqhkiG9w0BAQQFADA0MQswCQYDVQQGEwJVUzEO
MAwGA1UEChQFT1VSQ08xFTATBgNVBAMUDFNVUEVSRFVQRVJDQTAeFw05OTA1MTEx
ODM5MTZaFw0wMjA1MTAxODM5MTZaMFgxCzAJBgNVBAYTAlVTMRMwEQYDVQQIFApD
```

```
QUxJRk9STklBMQ4wDAYDVQQKFAVPVVJDTzEOMAwGA1UECxQFU0FMRVMxFDASBgNV
BAMUC09VUkNPU0VSVkVSMHwwDQYJKoZIhvcNAQEBBQADawAwaAJhALJolPnUTIsg
1fUNNHddMI0cx+qLbj6MhZ+4a+lufckCvS6yMr6AWiW2luQUUXf+iHG5XRxvOcQX
NVGYVHx04c1HkL7JYdwuEz27vH3iPIxB1sCH3J5jXZ2KSPBbf9yAqwIDAQABMA0G
CSqGSIb3DQEBBAUAA4GBAHOoo8W80J4btLNTCLyKKa0Mac9T6bv4YlupJQu8TUbC
aYSnH4TgyGNCO81CN3E5Wu4MbA2qCxMBJrS8QFiF6163mZSYQ/fY7V9ym7giXe3L
tgCrhPWnaNM2qrEu9KHXL/sQc1Y5J0vfq5nL/oRybAzzz8M/ukNY9lM8Vbmt4+dR
-----END CERTIFICATE-----
```

Transfer this data to a file called: `/export/home/inetmail/ourcoserver.cert` Be sure to include the `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` lines.

5. **Next, install the server certificate produced by the external Root CA...**

```
% /usr/bin/skistore -c /export/home/inetmail/ourcoserver.cert -k
'CN=OURCOSERVER, OU=SALES, O=OURCO, ST=CALIFORNIA, C=US'
/usr/bin/skistore: certificate
/export/home/inetmail/ourcoserver.cert successfully stored
/usr/bin/skistore: Operation Completed
```

6. **Next, install the Root CA certificate provided by the external CA...**

```
% /usr/bin/skistore -c /usr/http/certs/VerisignCA.cert -k
'OU=SECURE SERVER CERTIFICATION AUTHORITY, O=RSA DATA SECURITY,
INC., C=US'
/usr/bin/skistore: certificate /usr/http/certs/VerisignCA.cert
successfully stored

/usr/bin/skistore: Operation Completed

% /usr/bin/keypkg -Ah /usr/http/certs/VerisignCA.cert
/usr/bin/keypkg: Trusted key(s) successfully added
```

It should now be possible to make connections to the SSL-enabled IMAP and POP ports.

SSL Troubleshooting

How to Uninstall Server Credentials

If for some reason you suspect the validity of the server credentials, they may be removed from the SKI repository on the server machine using the following commands:

```
*** On the server machine:

# su root

# skicert -Reh
# keypkg -Dh
```

This deletes the server certificate and key package from the SKI repository.

How to Uninstall a Root CA Certificate on a Server Machine

It is possible that a Root CA certificate may expire, and that it will be necessary to remove it from the SKI repository on the server machine. This may be accomplished using the following commands.

```
*** On the server machine:

# su root
# keypkg -Rhs -t <rootca-dn>
# skicert -R -k <rootca-dn>
```

This removes the Root CA public key from the trusted key list in the server's key package and removes the Root CA certificate from the SKI repository.

How to Quit SSL Installation and Start Over

Because SSL installation must be absolutely perfect, it is sometimes best to simply quit and start from the beginning if you are having any doubts or problems with your initial installation. The following instructions will completely re-initialize the SKI repository on the machine on which they are run. Note that if the following commands are performed, ALL information pertaining to key packages and certificates will be lost, including any information maintained by a local Root CA:

```
# su root
# /etc/init.d/skiserv stop
# rm -rf /var/fn
# /etc/init.d/skiserv start
```

Note – Certain information pertaining to printer configuration may be lost as well.

CHAPTER 11

SIMS Periodic Maintenance Procedures

This chapter describes tasks that are performed on a regular basis, either scheduled or as needed.

TABLE 11-1 SIMS Maintenance Tasks

Topic/Task	Description	Page
IMTA Maintenance	- Adjusting Post Job Frequency - Adjusting the Frequency of the Return Old Messages Program	232
Sun Message Store Maintenance	- Recommended Maintenance Schedule - Message Purge - Message Store Backup and Restore - Message Store Data Check - Importing /var/mail Users - Deleting Old Messages - Deleting the User	234
Periodic Maintenance for the Sun Directory Services	- Maintaining the Data Store Attribute Indexes - Backing Up the Directory Data Base - Backing Up and Restoring Directory Service Configuration	246

IMTA Maintenance

Adjusting Post Job Frequency

The IMTA runs a periodic job called post.sh every four hours by default. The post.sh program scans through all the channels currently defined in the configuration file and checks the corresponding queues for messages. Processing jobs are unconditionally submitted to run the master channel programs for any channels, with master programs so as to poll remote systems that cannot establish their own connections. Jobs are also submitted for channels that support master channel programs and have messages queued. After this is done post.sh then terminates. It will run again in another four hours.

The post.sh program is the shell script, /opt/SUNWmail/imta/lib/post.sh, which the cron daemon is normally scheduled to run every four hours. IMTA's suggested default behavior of running the periodic delivery job once every four hours is appropriate for most sites. Indeed, at busy sites, running the periodic delivery job too frequently tends to be counterproductive.

If a site has a special need to run post.sh more frequently, they can change the crontab. Note, however, that RFC 1123, Requirements for Internet Hosts requires that Internet mail wait at least 30 minutes before being retried. Do not run your channel to the Internet more frequently than every half hour.

Finally, IMTA normally performs some periodic cleanup tasks when post.sh runs. IMTA's defaults are tuned for the case where the periodic job only runs every couple of hours. If you will be running the periodic job more frequently, you should adjust IMTA's cleanup task frequency: the IMTA_SYNCH_CACHE_PERIOD and IMTA_VERSION_LIMIT_PERIOD IMTA tailor options should be set to integer values so that these tasks are still performed only every couple of hours or so. (Refer to *SIMS Reference Manual* for more details on these strings.)

Adjusting the Frequency of the Return Old Messages Program

The IMTA runs a second periodic job called return.sh which has as its primary job the returning of old, undeliverable messages which have sat around in the message queues for too long. The return.sh shell script is at /opt/SUNWmail/imta/lib/return.sh. The cron daemon normally schedules it to run once a day at 30 minutes after midnight.

The return.sh scans the channels listed in the configuration file, checking the values established with the notices keyword. The messages queued to each channel are then checked. A warning message is sent for every message whose age in days matches any of the values specified with the notices keyword on the associated channel. The default ages if no notices keyword is specified for 3, 6, 9, and 12 days. If the message is as old or older than the final notices value, the entire message is returned and the original message is deleted from the channel queue; no further attempts to deliver the message will be made. (See the *SIMS Reference Manual* for notices channel keyword.)

The text of the warning and failure notices issued by the message return system is contained in the pair of files return_warning.txt and return_failure.txt located in the /opt/SUNWmail/imta/locale/{C}/LC_MESSAGES directory. These files can be edited to provide different notification text if desired.

IMTA maintains a history of delivery attempts for each message, which sometimes will include information about why the delivery attempts failed. This information is included in returned messages if RETURN_DELIVERY_HISTORY is set to 1 in the IMTA Option file (this is the default). A value of 0 disables the inclusion of this information.

The imta_tailor file options can be used to control the periodicity of the various subfunctions of the message return system. The IMTA_RETURN_SYNCH_PERIOD option in /opt/SUNWmail/imta/imta_tailor controls queue synchronization; the IMTA_RETURN_PERIOD IMTA tailor file option controls the return of expired messages and the generation of warnings; and the IMTA_RETURN_SPLIT_PERIOD IMTA tailor file option controls splitting of the mail.log file. If any of these options is set to an integer value *N*, then the action associated with the tailor file option will only be performed every *N* times the message return job runs. The value of these options is taken to be 1 if the option is not specified in the IMTA tailor file.

If the IMTA return job is running once an hour, then the default will be to issue warning notices for messages which have remained undeliverable for 3, 6, or 9 hours. Message which have remained undeliverable for 12 or more hours are returned in their entirety to their sender and no further delivery attempts are made.

Note – When RETURN_UNITS=1, these defaults will result in mail being bounced much too soon; therefore, sites are strongly encouraged to use the notices channel keyword to set “bounce” ages in excess of 12 hours.

The return.sh also performs various IMTA periodic cleanup tasks tuned on the assumption that the return job will only be running once a day. When return.sh is run more frequently, various IMTA parameters should be adjusted accordingly. In particular, the IMTA_RETURN_SYNCH_PERIOD and IMTA_RETURN_SPLIT_PERIOD IMTA tailor file options should generally be adjusted so that these tasks are still performed only once a day. See the imta purge and imta cache-sync utilities in the *SIMS Reference Guide* for details on the cleanup programs used.

Sun Message Store Maintenance

The Sun Message Store contains the content of the email system—messages and attachments. This section describes the maintenance procedures for the Sun Message Store. TABLE 11-2 summarizes the maintenance utilities provided for the Sun Message Store.

TABLE 11-2 Sun Message Store Maintenance Utilities

Utility	Description	Supported Interface/Reference
Purge	Removes messages that are no longer referenced in user and group folders and returns space to the Sun Message Store file system.	Admin Console. See “Configuring Purge Options” on page 173 and “To Configure the Purge Schedule” on page 175.
Backup	Copies contents of folders to specified backup device. Can perform full or incremental backups of all folders or the folder of a specified user or group.	Command-line utility (imbackup). See “Message Store Backup and Restore” on page 237.
Restore	Restores contents of all folders or one specified user or group folder from the backup device to the Sun Message Store.	Command-line utility (imrestore). See “Message Store Backup and Restore” on page 237.
Message Store data check	Scans through the Sun Message Store and the user folders verifying links.	Command-line utility (imcheck).
Import mailbox	Imports existing user’s mailbox in to the Sun Message Store.	Command line utility (imimportmbox).

TABLE 11-2 Sun Message Store Maintenance Utilities *(Continued)*

Utility	Description	Supported Interface/Reference
Delete user	Deletes the following from the Sun Message Store: Inbox, private folders, and private shared folders of a specified user; and public shared folders.	Command-line utility (imdeluser). Refer to "Deleting the User" on page 246.
Reinitialize user quota	Reinitializes a user's quota file in the user admin directory /usr/<hash number>/<username>/Adm.	Command-line utility (iminitquota). Refer to "To Activate Message Store Quota Enforcement on an Installed System" on page 163.
BackUp/Restore Message Store Configuration	Back up or restore Message Store Configuration	Admin Console. See "Message Store Configuration Backup and Restore" on page 158.
Deleting old messages	Deleting messages of a specified age.	Command-line utility (imexpire). Refer to "Deleting Old Messages" on page 245.

Some of the maintenance utilities impose a session-locking mechanism to prevent certain other maintenance utilities from being run in parallel. TABLE 11-3 outlines which utilities cannot run in parallel.

TABLE 11-3 Maintenance Utilities Session Locking

Utility	impurge	imbackup	imrestore	imimportmbox	imdeluser	imcheck	iminitquota	imexpire
impurge	Lock	Lock	Lock	Lock	Lock	Lock		Lock
imbackup/Solstice Backup	Lock				Lock			Lock
imrestore	Lock		Lock		Lock			Lock
imimportmbox	Lock				Lock			Lock
imdeluser	Lock	Lock	Lock	Lock	Lock		Lock	Lock
imcheck	Lock					Lock		Lock
iminitquota/update_quota dirsync					Lock		Lock	
imexpire	Lock	Lock	Lock	Lock	Lock	Lock		Lock

`imcheck` should not be run with any other utilities.

Recommended Maintenance Schedule

TABLE 11-4 outlines the recommended maintenance schedule for the Sun Message Store.

TABLE 11-4 Recommended Sun Message Store Maintenance Schedule

Task	Frequency
Full backup	Once per week
Incremental backup	Daily
Purge	Daily
Message Store data check	At least once per week or as needed
Restore	As needed
Importing user's folders and messages from `/var/mail` to the Sun Message Store	As needed
Delete user	As needed
Reinitialize user quota	As needed

Message Purge

When a message is delivered into the Sun Message Store, a reference is created in the Inbox of each of the message recipients. The reference points to the stored message. As each recipient reads, deletes, and removes (expunges) the message via their respective mail clients, the associated reference to the message is removed. When all references are removed, the message can be purged from the Sun Message Store.

The purge utility removes messages no longer referenced from any user or shared folder and returns the space to the Sun Message Store file system. The purge utility removes unreferenced messages starting with mail two days old and older. It does not remove unreferenced messages in today's and yesterday's mail. You must use the purge utility periodically; otherwise, the size of the Sun Message Store will grow unbounded.

For information on the other maintenance utilities with which purge can run concurrently, refer to TABLE 11-3.

You can invoke the purge utility by issuing the `impurge` command (see the *SIMS Reference Manual* and "To Configure the Purge Schedule" on page 175*)*, or you can configure purge options and a purge schedule using the Admin Console.

Message Store Backup and Restore

SIMS allows you to backup and restore the message store with a great deal of flexibility:

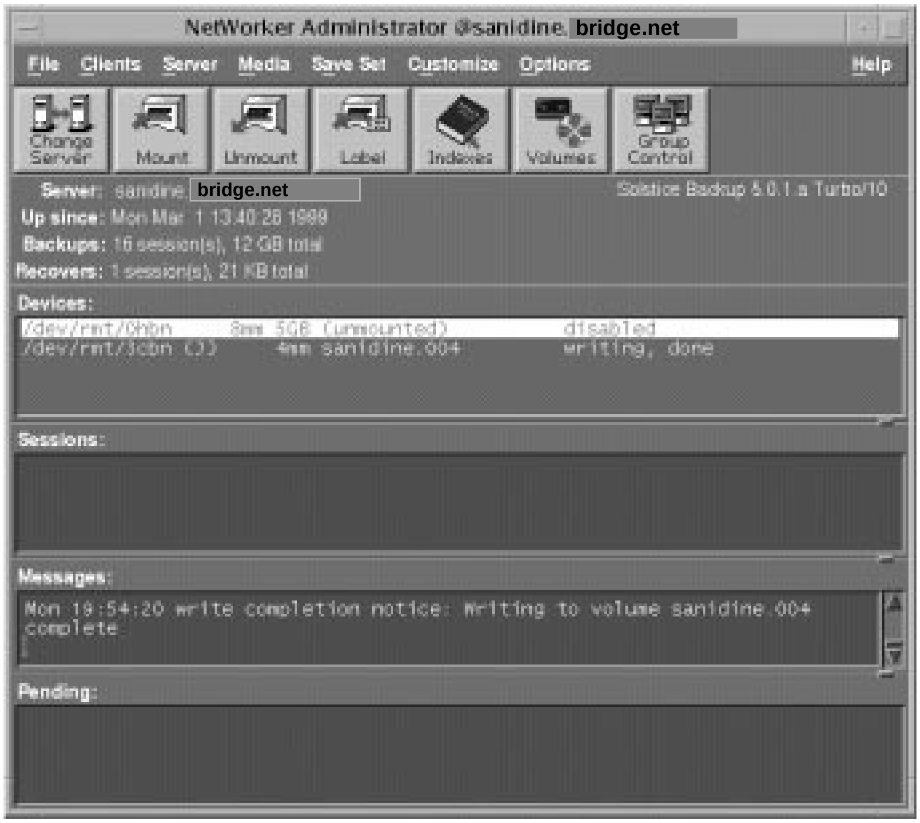
- You can backup and restore various parts of the message store. For example, you can backup all the mailboxes in the message store, the mailboxes of groups of users, the mailboxes specific users, or individual mail boxes.
- You can do concurrent backups of various parts of the message store. For example, if your message store is very large with many users, you can create groups of user mailboxes, and backup multiple groups on multiple devices concurrently.
- You can do full backups (backing up entire mailboxes) or incremental backups (backing up only the changes since the previous backup).

We recommend using Solstice Backup, a file backup and restore product that is part of the Solstice System Management Suite, to backup the SIMS message store. If you do not have Solstice Backup, use the command line utilities `imbackup` and `imrestore`. See `http://docs.sun.com` for documentation on Solstice Backup.

Note that Solstice Backup and the Legato Networker product are identical. The instructions here are applicable to both products. Read the Solstice Backup or Legato Networker documentation set before attempting to backup the message store.

Note – Do not use `ufsdump` to backup the message store.

Note – Message store backup and restore cannot run at the same time as some other maintenance utilities. Refer to TABLE 11-3 for session locking information.



Server: sanidine. bridge.net

Solstice Backup 5.0.1.a Turbo/10

Up since: Mon Mar 1 13:40:28 1999

Backups: 16 session(s), 12 GB total

Recovers: 1 session(s), 21 KB total

Devices:

```
/dev/rmt/0hbn      8mm 5GB (unmounted)          disabled
/dev/rmt/3cbn (J)      4mm sanidine.004          writing, done
```

Sessions:

Messages:

```
Mon 19:54:20 write completion notice: Writing to volume sanidine.004
complete
```

Pending:

FIGURE 11-1 Solstice Backup/Legato Networker.

Message Store Backup and Restore—Theory of Operation

The SIMS message store is not structured in a hierarchical file system by user and mailbox. However, in order to backup and restore user mailboxes with Solstice Backup, the message store mailboxes **need** to be created up in a hierarchical file system by user and mailbox. This is accomplished by running `mkbackupdir`, which creates a dummy directory tree reflecting the desired hierarchical file system. Note that using the command line utility `imbackup` does not require using `mkbackupdir`.

Note – `mkbackupdir` only creates a directory tree showing the user/mailbox hierarchy. This directory tree does NOT contain the message store data.

This hierarchy is used to structure the message store into a hierarchical file system with each mailbox consisting of a file. The files in this hierarchy are empty, and only used to provide this hierarchical information to Solstice Backup. If the directory already exists, `mkbackupdir` synchronizes the directory structure with the current folder/mailbox hierarchy.

The directory created by `mkbackupdir` is structured as follows:

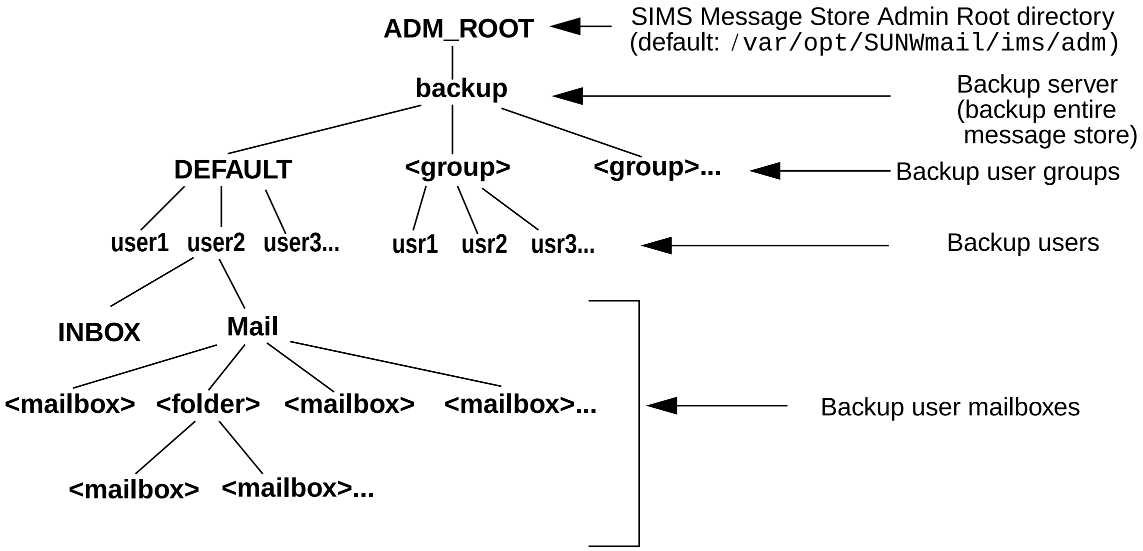


FIGURE 11-2 Solstice Backup Message Store Hierarchy.

Each of the nodes in the directory represents a set of mailbox files which can be saved by Solstice Backup.

- ADM_ROOT is the administration root directory defined in `/etc/opt/SUNWmail/ims/ims.cnf`. By default the directory is `/var/opt/SUNWmail/ims/adm/`.
- backup is the top-level node of the message store hierarchy. To back up all the message data at once on a single Solstice Backup Save Set, set the Client Save Set to this directory. Example: `/var/opt/SUNWmail/ims/adm/backup`
- groups are optional directories under which user mail folders can be grouped. For example, you may wish to group all the mailboxes of users with the login name starting with the letter *a* in a group called `A-group`, users with the login name starting with the letter *b* in a group called `B-group`, and so on. Groups can be used by both Solstice Backup and `imbackup`.

  Creating groups is useful for scheduling simultaneous backups of multiple save sets on multiple devices. By breaking up a particularly large message store into groups and setting up concurrent backups, you can reduce the amount of time it takes to backup a large message store. Breaking your message store into groups also allows you to backup part of the message store instead of the entire message store. If you do not create any groups, all folders are saved under a directory called DEFAULT and you cannot perform concurrent or partial message store backups.

Groups can be created by manually modifying the default hierarchical directory created by mkbackupdir. Groups can also be created automatically by specifying a series of regular expressions which will divide users by name. These methods are described in "Full Message Store Backups Using Solstice Backup" on page 240.

- user directories contain the mailbox hierarchy for each mail user. Under each user directory is a file called INBOX which stores all incoming messages and a Mail directory containing the user's mailboxes and folders. (In this picture a mailbox is a file that holds messages, and a folder is a directory that hold mailboxes.)

Backup Choices and Recommendations

You have the following choices for backing up the message store using Solstice Backup:

1. You can choose to back up at any hierarchical level in the directory just like a file system. For example you can back up a mailbox, all of a single users mailboxes, the mailboxes of a group of users, or all the mailboxes in the entire message store.

2. You can divide your message store space into user groups and backup multiple groups concurrently.

3. You can perform a *full backup* (save all user mailboxes) or an *incremental backup* (save only mailboxes that have changed since a specified date).

We recommend that you perform a full backup every week, and an incremental backup every other day.

▼ Full Message Store Backups Using Solstice Backup

1. **If you decide to do concurrent backups or backup of groups of users as opposed to all the users in the message store, break your messages store into groups of users and create a hierarchical file system that reflects these groups. If you do not require groups of users, go to step 2.**

   Groups can be created manually or automatically. If you decide to create groups manually, skip to step 2. If you wish to create groups automatically, specify your groups in the /var/opt/SUNWmail/ims/backup.cnf file. The format for specifying groups is:

```
groupname: <user names>
```

where, `groupname` is the name of the directory under which the user and mailbox directories will be stored, and `<user names>` is a UNIX regular expression specifying user directory names that will go under the `groupname` directory.

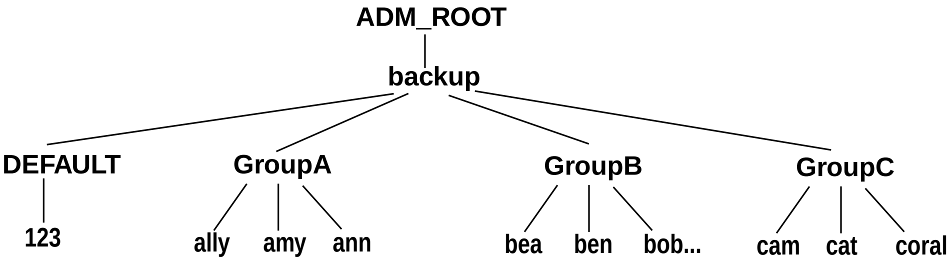
Example 1: You have the following message store users:

```
ally, amy, ann, bea, ben, bob, cam, cat, coral, 123
```

The following entries in `backup.cnf` will create three group directories called `groupA`, `groupB`, and `groupC`. Below these `group*` directories will be user directories corresponding to the user names beginning with a, b, and c (usernames are not case-sensitive):

```
groupA: ^a.*
groupB: ^b.*
groupC: ^c.*
```

The directory structure will look like this:



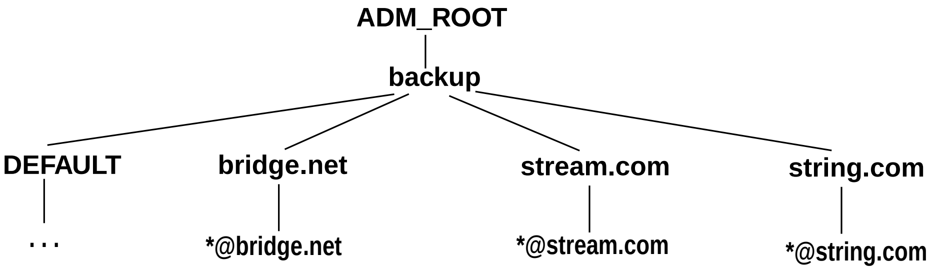
Create groups that are approximately equal in size so that backing up for each one take about the same amount of time.

Example 2: Use the following `backup-groups.cnf` file to create backup groups of users in domains `stream.com`, `bridge.net`, and `string.com`:

```
backup-groups.cnf:

bridge.net: .*@bridge.net$
stream.com: .*@stream.com$
string.com: .*@string.com$
```

The directory structure will look like this:



2. **Run `mkbackupdir` at the command line.**

   `mkbackupdir` creates a directory tree showing the user folder hierarchy. **This directory tree WILL NOT contain the message store data—even after running Solstice Backup.** The files in this hierarchy are only to provide hierarchical file information to Solstice Backup. If the hierarchical directory already exists, `mkbackupdir` synchronizes the directory with the current folder/mailbox hierarchy.

3. **(Optional) Create user groups manually.**

   If you have created groups automatically (Step 1) or if you do not want to create groups, skip to step 4. If you want to create groups manually use the `mkdir` command to create group directories under `/var/opt/SUNWmail/ims/adm/backup`. Each directory should be a group name.

   Example:

   After your group directories are created, manually move the user directories under `/var/opt/SUNWmail/ims/adm/backup/DEFAULT` to the desired group directories.

4. **Start Solstice Backup.**

   Do not use the Solstice Backup incremental backup feature. To do an incremental backup see "Incremental Message Store Backup Using Solstice Backup" on page 244. Specify concurrent backups as necessary.

Note – The `.nsr` files are generated by the `mkbackupdir` command. It contains standard Networker directives and should never be edited.

---

5. **Automate this procedure.**

   The preceding steps describe how to run Solstice Backup manually. We recommend that you set up a cron job to run mkbackupdir every week and then use the Solstice Backup GUI to schedule backups after mkbackupdir is run. (Instead of setting up a cron job, you can also specify mkbackupdir as a Backup Command in the Solstice Backup program).

▼ Full Message Store Backups Using imbackup

1. **If you decide to do concurrent backups or backup of groups of users as opposed to all the users in the message store, break your messages store into groups of users. If you do not require groups of users, go to step 2.**

   Groups can be created manually or automatically. If you wish to create groups automatically, specify your groups in the /var/opt/SUNWmail/ims/backup.cnf file. The format for specifying groups is:

   ```
   groupname: <user names>
   ```

   where, groupname is the name of the directory under which the user and mailbox directories will be stored, and <user names> is a UNIX regular expression specifying user directory names that will go under the groupname directory.

   Example 1: Use the following imbackup command with the following backup-groups.cnf file to backup all the users whose uid starts with the letter "a":

   ```
   # imbackup -g groupA
   ```

   ```
   backup-groups.cnf:
   ```

   ```
   groupA: ^a.*
   groupB: ^b.*
   groupC: ^c.*
   ```

   Example 2: Use the following imbackup command with the following backup-groups.cnf file to backup all the users in domain stream.com:

   ```
   # imbackup -g stream.com
   ```

   ```
   backup-groups.cnf:
   ```

   ```
   bridge.net: .*@bridge.net$
   stream.com: .*@stream.com$
   string.com: .*@string.com$
   ```

2. **Run imbackup.**

▼ Incremental Message Store Backup Using Solstice Backup

A full backup saves the user’s current mailbox. An incremental backup saves changes to the mailbox from specified date.

1. **Set up a `cron` job or specify `mkbackupdir -d` as a Backup Command in the Solstice Backup program.**

   The proper format is:

   ```
   mkbackupdir -d <date (yyyymmdd) since last full backup>
   ```

   This will create an incremental backup directory hierarchy for only mailboxes that have been modified since a specified date. Solstice Backup will only backs up those mailboxes. For example, if you run a full backup using `mkbackupdir` on 1 January 2000, you can do one week incremental backup by running:

   ```
   mkbackupdir -d 20000108
   ```

▼ Restoring the Message Store

Utility: `imrestore`

You cannot use `imrestore` to restore mailboxes backed up with Solstice Backup, and you cannot use Solstice Restore to restore mailboxes backed up with `imbackup`. For more detailed information on how to use Solstice Restore and `imrestore`, refer to the Solstice Backup documents (`http://docs.sun.com`) or the `imrestore` man page.

If you use Solstice Backup to recover a message store, you will receive the message “File already exists. Do you want to overwrite, skip, backup, or rename?” Choose overwrite. This message appears because the backup tree is just the directory hierarchy, that is, it consists of empty files and stays that way permanently.

Note – If you use the Solstice `recover` command, then you can use the `-A` and `-iy` arguments to suppress this message.

Message Store Data Check

Utility: `imcheck`

The folder check utility scans through the Sun Message Store and the user folders verifying links. That is, it verifies that all the messages in the folders are accessible. In addition to running the folder check utility at regular intervals for maintenance, you can also run this utility after a system failure to ensure that all message deliveries were made while the system was in a questionable state. If the utility determines that messages are not in user folders and hence were not delivered, it will redeliver the messages.

You can invoke the folder check utility by issuing the `imcheck` command at a command-line interface. For information on the `imcheck` command, refer to the *SIMS Reference Manual*.

Importing `/var/mail` Users

Utility: `imimportmbox`

The import mailbox utility automatically imports an existing user's Inbox folder and all messages from `/var/mail` to the Sun Message Store. You must manually import a `/var/mail` user's private folders.

You can invoke the import mailbox utility by issuing the `imimportmbox` command at a command-line interface. For information on the `imimportmbox` command and importing `/var/mail` users refer to "Migrating /var/mail Mailboxes" on page 328 and the *SIMS Reference Manual*.

For information on the other maintenance utilities with which import mailbox can run concurrently, refer to TABLE 11-3.

Deleting Old Messages

Utility: `imexpire`

The `imexpire` command allows administrators to mark as permanently deleted or "expired" any user messages older than a specified date or older than a number of specified days. The deleted messages are expunged from the user mailbox when the user connects or disconnects from the server. The actual data is removed from the message store when `impurge` is run. Refer to the *SIMS Reference Manual* for further details.

▼ To Disable Automatic Quota Synchronization

If you want to change or disable the automatic quota synchronization (for example you need to do message store maintenance and you want the synchronization to occur), edit the following `crontab` entry:

```
10,30,50 * * * * [ -x /opt/SUNWmail/imta/sbin/imta ] && /opt/
SUNWmail/imta/sbin/imta dirsync -C /opt/SUNWmail/lib/
libquota.so.1:update_quota:5
```

Deleting the User

Utility: `imadmin-delete-user`

To delete a user's entry and mailbox, use `imadmin-delete-user`. (See "To Delete a User or Group Entry from the Directory" on page 41.) To remove only the user mailbox and not the user entry in the directory, use the `imdeluser` command.

Periodic Maintenance for the Sun Directory Services

Note – You will need the *Sun Directory Services 3.1 Administration Guide* for more details on some of these tasks.

Maintaining the Data Store Attribute Indexes

When entries are deleted, they still occupy space in the directory database. Regenerate the attribute index periodically to retrieve this space.

Note – Regenerating a large database can take a considerable amount of time (2-5 hours for 50,000 entries depending upon the system configuration). During regeneration users cannot log into their mailboxes, although mail is still delivered to mailboxes.

You can regenerate the attribute index by using the Sun Directory Services Admin Console. You need to do this for each data store individually. Refer to the *Sun Directory Services 3.1 Administration Guide* for details. Alternatively, you can use the `idxgen` command to regenerate indexes. Refer to the `dsidxgen` man page for more information.

Note – If you add any additional index definitions to `dsserv.conf`, you must regenerate the indexes before running `dsservd` again. This is true even if you have not yet added data matching the new indexes to the Directory.

Backing Up the Directory Data Base

The directory data base is stored in a binary format called LDBM. Back up the LDBM database by using the LDBM Data Store backup feature in the Sun Directory Services Admin Console (see the *Sun Directory Services 3.1 Administration Guide)* or simply backup LDBM database files using the `tar` command. The location of the LDBM database files is defined by the `directory` parameter in `/etc/opt/SUNWconn/ldap/current/dsserv.conf`. Before using the `tar` command on these files, put the directory in the read-only mode so LDBM database files don’t get written to during backup.

Because the LDBM database is stored in binary files, they cannot be properly restored if the files themselves are corrupted. For this reason you may also choose to backup the directory database in the text-based LDIF format. You can make LDIF backups of your LDBM directory database by using the command `ldbmcat`. To restore the LDIF database files back to LDBM, use the command `ldif2ldbm`. Refer to the man pages for more information.

Backing Up and Restoring Directory Service Configuration

Use the Backup Configuration feature in the Sun Directory Services Admin Console (see the *Sun Directory Services 3.1 Administration Guide)* to backup the directory service configuration file. This is particularly important if you change the Sun

Directory Services configuration from the default. The Sun Directory Services Admin Console also provides a configuration restore feature to restore any of your backed up directory service configurations.

CHAPTER 12

SIMS Monitoring and Logging

Monitoring enables you to manage your SIMS server more effectively. Through monitoring, problems are detected earlier so that you can take corrective actions before your mail service is affected.

SIMS provides a number of ways of monitoring the messaging components. The three primary ways are:

1. Monitoring utilities
2. SNMP support
3. Log files

In addition, there are several categories of information that you can monitor, these include:

- Availability: Is a service or component operating?
- Connectivity: Is the mail service accessible? (POP, IMAP etc.)
- Response time: How is the service performing from an end user perspective?
- Processes: Are critical processes running?
- Resources: Is there sufficient disk space for the message store? Is there enough virtual memory? What is the system load?
- Security: Are there denial of service attacks in progress? Is the service subject to a SPAM attack? If so, from where?

The monitoring capabilities built into SIMS allow you to answer these questions. This chapter explains how to monitor a SIMS based e-mail service, and how to automate the monitoring process so that you are notified as problem situations that need attention develop.

Logging Facilities

SIMS captures a lot of information about significant events in the operation of the email service. This information is logged to various log files that are listed in TABLE 12-3. The type of information that is collected can be controlled. Some components provide a configuration file where the logging detail can be set (refer to the appropriate section in the *SIMS Reference Manual*).

Since an active SIMS server can generate a lot of logging information, manual analysis of the log files is often impractical. For this reason, SIMS includes a number of monitoring tools that extract interesting statistics from the log files (see “SIMS Monitoring Utilities” on page 261). In addition useful analysis can be performed using Solaris shell scripts. For example, here’s how to determine the number of successful IMAP logins today:

```
% grep -c "ims.imaccessd\[[0-9]*\]\: imap\[[0-9]*\]\: Auth" /var/
log/syslog
252
```

and how to determine how many IMAP connections were lost:

```
% grep -c "ims.imaccessd\[[0-9]*\]\: imap\[[0-9]*\]\: Connection
broken" /var/log/syslog
13
```

Message Store / Message Access Log Files

he MSMA logs all `imaccessd` and message store utility errors and events. Log messages are in the `/var/log/syslog` file and prefixed with `SUNWmail.ims`. Note that system messages are logged every time a user checks for mail. It logs the pop3 and imap login and logout. This can cause a clutter syslog messages. To stop login / logout messages from clogging you syslog file, change the syslog logging level in /etc/syslog.conf from mail.debug to mail.notice and restart the syslog daemon after the change. See the syslog(3) man page for details.

Sun Directory Service Log Files

If configured, logs various information such as protocol trace information for function calls and debug information about packets. Log files are in the /var/opt/SUNWconn/ldap/log directory and are shown in TABLE 12-1. Refer to Netscape Directory Service documentation for information on Netscape log files.

Note – Note that if you are using the Netscape Directory Service, the log files will be different. Refer to product documentation.

TABLE 12-1 Overview of Sun Directory Service Logging Files

Log File	Description	Further Information
dsserv.log	Directory events	Sun Directory Services documentation
dsweb.log.log	Directory Web Gateway events	Sun Directory Services documentation
dsnmpserv.log	Directory SNMP events	Sun Directory Services documentation

By default, the directory server daemon logs information about connections and operations in /var/opt/SUNWconn/ldap/log/dsserv.log. In the event that you need more diagnostic ability than is provided by SIMS default Directory configuration, you may run dsservd from a shell manually, providing additional diagnostics. See the -d and -s arguments to dsservd, documented in dsservd(8) man page. Note that running with additional diagnostics turned on will run dsservd in the foreground, and will use up disk space quickly if you have all optional diagnostic output enabled.

In addition, certain messages may be logged to the console of the machine on which dsservd is running, and/or to /var/adm/messages.

TABLE 12-2 contains an example of the information that is logged during a search operation. This example shows two interactions with the directory, the first to add an entry, and the second to search the directory for all entries that have a commonName attribute. The log includes details of the bind and unbind, and operational information.

TABLE 12-2 `dsserv.log` Example

```
Thu May 15 16:03: conn=9 fd=15 connection from unknown (127.0.0.1)
Thu May 15 16:03: conn=9 op=0 BIND dn="CN=admin,O=sun,C=us" method=128
Thu May 15 16:03: conn=9 op=0 RESULT err=0 tag=97 nentries=0
Thu May 15 16:03: conn=9 op=1 ADD dn="O=sun,C=us"
Thu May 15 16:03: conn=9 op=1 RESULT err=0 tag=105 nentries=0
Thu May 15 16:03: conn=9 op=2 UNBIND
Thu May 15 16:03: conn=9 op=2 fd=15 closed errno=0
Thu May 15 16:26: conn=10 fd=15 connection from unknown (127.0.0.1)
Thu May 15 16:26: conn=10 op=0 BIND dn="CN=admin,O=sun,C=us" method=128
Thu May 15 16:26: conn=10 op=0 RESULT err=0 tag=97 nentries=0
Thu May 15 16:26: conn=10 op=1 SRCH base="O=sun,C=us" scope=2 filter="(cn=*)"
Thu May 15 16:26: conn=10 op=1 RESULT err=0 tag=101 nentries=150
Thu May 15 16:26: conn=10 op=-1 fd=15 closed errno=0
Thu May 15 16:26: conn=10 op=2 UNBIND
```

IMTA Log Files

If configured, an IMTA channel logs in each email as it enters and is removed from the channel queue. Unless otherwise indicated in the table below, IMTA log file names are located in the directory `/var/opt/SUNWmail/imta/log`.

TABLE 12-3 Overview of IMTA Logging Files

Log File	**Description**	**Further Information**
mail.log	Cumulative IMTA events	"Diagnostics Output" on page 105, "Message Logging" on page 107 "Logging Messages Passing Through the IMTA" on page 254 "Viewing Enqueued Messages" on page 116
mail.log_current	Today's IMTA events	"Logging and Tracking Messages in the IMTA" on page 253
mail.log_yesterday	Yesterday's IMTA events	"Logging and Tracking Messages in the IMTA" on page 253
dispatcher.log-*	SMTP dispatcher	*SIMS Reference Manual*: log files. IMTA service dispatcher
job_controller.log-*	Job controller	*SIMS Reference Manual*: job controller
tcp_smtp_server.log-*	SMTP server	"Check Processing Log Files" on page 281
/var/log/syslog	prefixed with SUNWmail.imta	"Troubleshooting the IMTA" on page 278

TABLE 12-3 Overview of IMTA Logging Files *(Continued)*

Log File	Description	Further Information
channel_master.log-*	Master program output (usually client) for channel	"Troubleshooting the IMTA" on page 278
channel_slave.log-*	Output of slave program (usually server) for channel	"Troubleshooting the IMTA" on page 278
server-name_server.log-*	Logging for server server-name	"Troubleshooting the IMTA" on page 278
server-name_thread.log-*	Per thread errors for server-name	"Troubleshooting the IMTA" on page 278
post.log-*	Log output for the periodic IMTA delivery job	"Troubleshooting the IMTA" on page 278
return.log-*	Log output for the periodic IMTA message bouncer job	"Troubleshooting the IMTA" on page 278

Channel log files are not created unless an error occurs or debugging output is enabled for the channel with the `master_debug` channel keyword or `slave_debug` channel keyword.

Each new log file is created with a unique id to avoid overwriting an earlier log written by the same channel. You can use the `imta find` utility to aid in finding the desired "version" of a log file. You can purge back older log files using the `imta purge` command.

Logging and Tracking Messages in the IMTA

This section points out some message logging and tracking techniques.

Identifying the Source of Incoming SMTP Messages

When the identtcp or identtcpnumeric channel keyword is set in the tcp_local channel, the IMTA attempts to use an IDENT query to identify incoming SMTP connections. If the sending system is running an IDENT server, it will return to the IMTA the SMTP sender's identity for the IMTA to insert in the Received: header the IMTA constructs. If the sending system is not running an IDENT server, the IMTA will just use the port number (port 25) and the sending system IP address or name.

With identtcpnumeric, the IMTA uses the IDENT information (if any) and the actual IP address of the sending system; with identtcp, the IMTA also attempts to translate the IP address to a system name by performing a DNS reverse lookup.Thus identtcpnumeric incurs slightly less overhead because it does not do the DNS reverse lookup, and the actual IP address might be considered somewhat more authoritative that the name resulting from a DNS query. However, using the system name as with identtcp may be considered more user-friendly.

Identifying information in Received headers can assist in detecting spoofed email and in holding the senders of such spoofed email accountable. Note that user friendly identifying information is a not insignificant feature: even a naive user may notice that a Received header in a suspicious message contains an unexpected address, for example, anonymous@SpoofersAreUs.edu, but only a fairly sophisticated user is able to pay attention to any IP addresses showing up in Received headers. So a choice between these keywords may be affected by whether you are looking to provide forewarning to users that they may have received spoofed email, or whether you merely wish to preserve the identifying information for use in investigating cases of spoofed email.

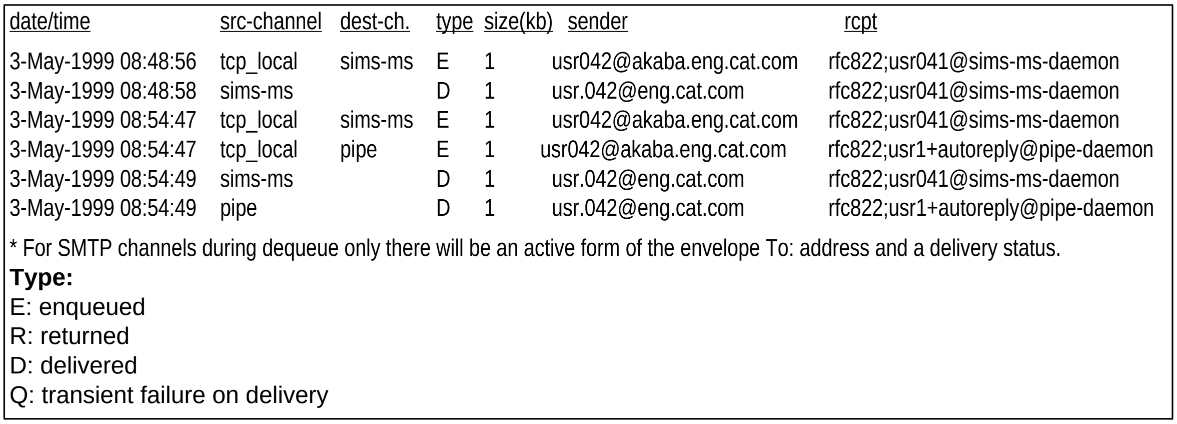
Logging Messages Passing Through the IMTA

The IMTA provides facilities for logging each message as it is enqueued and dequeued. All log entries are made to the mail.log_current file in the IMTA log directory, /var/opt/SUNWmail/imta/log. Logging is controlled on a per-channel basis. The logging keyword activates logging for a particular channel while the nologging keyword disables it. Logging is enabled on all channels by default.

When logging is turned on, the cumulative mail.log file in the IMTA log directory will continue to grow and it is up to you to periodically write it to backup and delete it, or truncate it, or whatever your site prefers.

The log file is written as normal ASCII text and the format is quite simple. By default, each entry contains eight or nine fields. An example is shown in the

CODE EXAMPLE 12-1 `mail.log_current` File.



```
date/time             src-channel  dest-ch.  type size(kb) sender                    rcpt

3-May-1999 08:48:56   tcp_local    sims-ms   E    1        usr042@akaba.eng.cat.com  rfc822;usr041@sims-ms-daemon
3-May-1999 08:48:58   sims-ms                D    1        usr.042@eng.cat.com       rfc822;usr041@sims-ms-daemon
3-May-1999 08:54:47   tcp_local    sims-ms   E    1        usr042@akaba.eng.cat.com  rfc822;usr041@sims-ms-daemon
3-May-1999 08:54:47   tcp_local    pipe      E    1       usr042@akaba.eng.cat.com   rfc822;usr1+autoreply@pipe-daemon
3-May-1999 08:54:49   sims-ms                D    1        usr.042@eng.cat.com       rfc822;usr041@sims-ms-daemon
3-May-1999 08:54:49   pipe                   D    1        usr.042@eng.cat.com       rfc822;usr1+autoreply@pipe-daemon

* For SMTP channels during dequeue only there will be an active form of the envelope To: address and a delivery status.
Type:
E: enqueued
R: returned
D: delivered
Q: transient failure on delivery
```

You can also view the message queue by running:

`% imta cache -view <channel_name>`

The `imta test -rewrite` command verifies that an address is properly handled by the IMTA.

If you still cannot find a lost message, check whether it's being held, by looking for `*.HELD` messages in the channel queues.

The fields are described in TABLE 12-4:

TABLE 12-4 Log File Fields

date/time	Date and time when the entry was made.
src-channel	Channel name for the source channel.
`dest-ch.`	Channel name of the destination channel. For SMTP channels when `LOG_CONNECTION` is enabled, a minus sign (`-`) indicates inbound to the SMTP server, a plus sign (`+`) indicates outbound via the SMTP client.
`Type`	Type of entry. See TABLE 12-5.
`Size`	Size of the message. This is expressed in kilobytes by default, although this default can be changed by using the `BLOCK_SIZE` keyword in the IMTA option file.

TABLE 12-4 Log File Fields *(Continued)*

`Sender`	Envelope `From` address. Note that for messages with an empty envelope `From` address, such as notification messages, this field will be blank.
`Rcpt`	Original form of the envelope `To` address.
`smtp:250<marlow@alpha.com>`	Active (current) form of the envelope `To` address (SMTP channels during dequeue only).
`Recipient ok`	Delivery status (SMTP channels only during dequeue).

The logging entry codes are described in TABLE 12-5:

TABLE 12-5 Logging Entry Codes

Entry	Description
General	
D	Successful dequeue.
E	Enqueue.
J	Access control mapping of attempted enqueue.
Q	Temporary failure to dequeue.
R	Recipient address rejected on attempted dequeue.
Z	Some successful recipients, but this recipient was temporarily unsuccessful; the original message file of all recipients was dequeued, and in its place a new message file for this and other unsuccessful recipients will be immediately re-enqueued.
SMTP Channels' LOG_CONNECTION + or - entries	
C	Connection closed.
O	Connection opened.
X	Connection rejected.
Y	Connection try failed before being established.

Extra Logging Detail

In addition to the base set of logging enabled by the `logging` channel keyword, the IMTA has options that cause additional information to be included in the entries written to the `mail.log*` files. Note that logging such additional information tends to incur additional overhead.

Particularly likely to be of interest are the LOG_MESSAGE_ID, LOG_FILENAME, and LOG_CONNECTION options. Enabling LOG_MESSAGE_ID allows correlation of which entries relate to which message.

Enabling LOG_FILENAME makes it easier to immediately spot how many times delivery of a particular message file has been retried, and can be useful in understanding when the IMTA does or does not split a message to multiple recipients into separate message file copies on disk.

Enabling LOG_CONNECTION causes the IMTA to log TCP/IP connections, as well as message traffic, to the mail.log files by default; alternatively, the SEPARATE_CONNECTION_LOG option may be used to specify that connection log entries instead be written to connection.log files. That is, if SEPARATE_CONNECTION_LOG and LOG_CONNECTION are set, the connection log entries will be written to the connection.log_current file in the IMTA log directory.

Setting LOG_HEADER=1 may be of interest if you wish to save certain message headers to the mail.log* files.

Additionally, setting LOG_PROCESS=1 and LOG_USERNAME=1 on an IMTA firewall system generally results in fairly monotonous extra information being logged: the process ID of the process enqueuing a message on an IMTA firewall system would normally be that of an IMTA SMTP server process (for SMTP messages), and the user name would normally just be the user name of the user who last restarted the IMTA Service Dispatcher. Enable these options if you wish to confirm that the process IDs and user names of processes enqueuing messages are as expected.

Note – It is up to the individual sites whether or not to implement a log cleaning policy. By default, mail.log is never removed; this can potentially fill up your disk space.

Snapshots of Message Traffic through the IMTA

Command: imta-counters

The IMTA has channel statistics counters to collect and monitor channel counters based upon the SNMP Mail Monitoring MIB, RFC 1566. These counters tabulate on a per channel basis the twelve items described in TABLE 12-6.

TABLE 12-6 Channel Counters

Field name	Description
`received_messages`	The number of messages enqueued to the channel
`submitted_messages`	The number of messages enqueued by the channel
`stored_messages`	The total number of messages currently stored for the channel
`delivered_messages`	The number of messages dequeued by the channel
`received_volume`	Volume of messages enqueued to the channel as measured in IMTA kilobytes
`submitted_volume`	Volume of messages enqueued by the channel as measured in IMTA kilobytes
`stored_volume`	Volume of messages currently stored for the channel as measured in IMTA kilobytes
`delivered_volume`	Volume of messages dequeued by the channel as measured in IMTA kilobytes
`received_recipients`	Number of recipients specified in all messages enqueued to the channel
`submitted_recipients`	Number of recipients specified in all messages enqueued by the channel
`stored_recipients`	Number of recipients specified in all messages currently stored for the channel
`delivered_recipients`	Number of recipients specified in all messages dequeued by the channel
`next`	Pointer to the next list entry of channel counters.
`rejected_messages`	Count of messages which, upon trying to be enqueued to the channel, were rejected.
`failed_messages`	Count of messages enqueued to the channel which, when processed, failed to be delivered for one or more recipients owing to permanent errors of some sort (for example, invalid recipient address).
`attempted_messages`	Count of messages enqueued to the channel whose delivery has been attempted.
`rejected_volume`	Cumulative volume of messages which, upon trying to be enqueued to the channel, were rejected.
`failed_volume`	Cumulative volume of messages enqueued to the channel which, when processed, failed to be delivered for one or more recipients owing to permanent errors of some sort (for example, invalid recipient address).
`attempted_volume`	Cumulative volume of messages enqueued to the channel whose delivery has been attempted.

TABLE 12-6 Channel Counters *(Continued)*

Field name	Description
rejected_recipients	Cumulative count of recipient addresses which, upon trying to be enqueued to the channel, were rejected.
failed_recipients	Cumulative count of recipients enqueued to the channel which, when processed, failed to be delivered owing to permanent errors of some sort (e.g., invalid recipient address).
attempted_recipients	Cumulative count of recipients enqueued to the channel whose delivery has been attempted.
delivered_first_messa ges	Cumulative count of messages enqueued to the channel which were successfully delivered (or returned as undeliverable) on their first processing attempt.
delivered_first_queue _count	Cumulative count of first message delivery attempts made by the channel. When this value is less then *received messages*, it means that delivery has not yet been attempted for all received messages. This is not unusual: this value is expected to lag behind *received messages*.
delivered_first_queue _time	Cumulative count of elapsed seconds between when a message is enqueued and when processing of its first delivery attempt completes. The result of dividing *delivered first queue time* by *delivered first queue count* gives the average amount of time in seconds spent by a message in the processing queues as it awaits its initial delivery attempt.
deliveredqueue_count	Cumulative count of message delivery attempts made by the channel.
delivered_queue_time	Cumulative count of elapsed seconds between when a message is enqueued and when it is finally removed from the channel queue. The result of dividing *delivered queue time* by *delivered queue count* gives the average amount of time in seconds spent by a message in the processing queues.

It is important to note that these counters generally need to be looked at over time noting the minimum values seen. The minimums may actually be negative for some channels. Such a negative value merely means that there were messages queued for a channel at the time that its counters were zeroed (e.g., the cluster-wide database of counters created). When those messages were dequeued, the associated counters for the channel were decremented therefore leading to a negative minimum. For such a counter, the correct “absolute” value is the current value less the minimum value that counter has ever held since being initialized.

Purpose and Use of Counters

The IMTA channel counters are intended for indicating the trend and health of your e-mail system. The IMTA channel counters are not designed nor intended to provide an accurate accounting of message traffic. For precise accounting, see “Logging

Messages Passing Through the IMTA" on page 254. The IMTA's channel counters are implemented using the lightest weight mechanisms available, namely a shared memory section on each system.

Example of counters interpretation

The example below shows a sample excerpt of counters data, as might be seen using the `imta counters -show` utility.

```
Channel         Messages      Recipients      Blocks
-------         --------      ----------      ------
directory
   Received     6523          9042            69694     (1)
   Stored       4             4               149       (2)
   Delivered    6519          9038            69545     (3)
   Submitted    6811          9019            71123     (4)
```

In this example:

1. The "Received" value represents a count of messages coming from any channel to the channel named directory. That is, messages enqueued to the directory channel by any other channel.
2. The "Stored" value represents a count of messages stored in the channel queue to be delivered. This will generally correspond to the number of entries currently stored for the channel in the IMTA queue cache database.
3. The "Delivered" value represents a count of messages which have been processed (dequeued) by the channel directory; a dequeue operation may either correspond to a successful "delivery" (that is, an enqueue to another channel), or to a dequeue due to the message being returned to the sender. This will generally correspond to the number Received minus the number Stored.
4. The "Submitted" value represents a count of messages which have been enqueued from the channel directory to any other channel.

Note that in this example, the number of messages Submitted is greater than the number delivered. This is often the case, since each message the channel dequeues (delivers) will result in at least one new message enqueued (submitted) but possibly more than one. For example, if a message has two recipients reached via different channels, then two enqueues will be required. Or if a message bounces, a copy will go back to the sender and another copy may be sent to the postmaster. Usually that will be two submissions (unless both are reached through the same channel).

SIMS Monitoring Utilities

SIMS provides a set of command line monitoring tools (see TABLE 12-7) that provide detailed information about the status and performance of a SIMS server. For additional information refer to the man pages.

TABLE 12-7 SIMS Monitoring Commands

Command	**Component Monitored**	**Description**
`immonitor-queue`	IMTA	Displays the sizes of IMTA channel queues, domains for which there have been delivery problems.
`immonitor-access`	MSMA	Determines the responsiveness of the POP, IMAP and LDAP services and mail delivery round trip time.
`immonitor-system`	SIMS System	Monitors the status of the system resources: swap space, disk utilization and network status.
`immonitor-users`	IMTA	Provides a summary of the top mail submitter, useful for SPAM detection.
`immonitor-reenqueue`	IMTA	Allows messages to be moved from one channel to another to perform queue load balancing or to delay the delivery of messages to domains that are temporarily inaccessible
`imta-counters`	IMTA channel counters	Provides information about IMTA channel counters. Refer to the `imta-counters` man page and logging section of the *SIMS Reference Manual*.
`imta dispatcher_stats_tty`	SMTP	Outputs the current open incoming SMTP connections and by which SMTP server process they are handled. (no man page)

SIMS Monitoring Plan

The key attributes of a SIMS mail server that determine server performance are:

- **Message Transport Queue Size**. Messages passing through a SIMS server are stored in the IMTA message queues. The performance of the IMTA depends on the size of the queue. An extremely large Queue size can slow down the IMTA.

- **Accessibility and responsiveness of core SIMS services (SMTP, IMAP, POP, LDAP)**. A large number of connections (POP, IMAP, SMTP. LDAP) may indicate that connections are being abnormally terminated, either because of a failure of a SIMS service or a deliberate denial of service attack. Either of these can lead to reduced performance of the SIMS server.
- **System Resource Utilization**. Normal SIMS operation contributes to system load and resource consumption, such as cpu, disk and virtual memory resources. To keep SIMS performing at an optimal level it is important to monitor system resources.

To ensure high availability of the e-mail service, the key attributes of the system should be continually monitored. This will allow the system administrator to be alerted automatically whenever a potential problem develops. We recommend monitoring at least the attributes listed in TABLE 12-8.

Each monitoring utility allows thresholds to be set which define the upper bounds on the resource utilization, for example, the maximum amount of disk space used by the message store directory. When the threshold is exceeded, the utility can generate an alert or initiate the notification of a system operator via a pager (must be e-mail accessible). Establishing a reasonable set of thresholds depends on the performance characteristics of the system on which the component is running (e.g., low-end or high-end server) and the usage profile of your e-mail service. TABLE 12-8 shows some example default thresholds settings that we recommend monitoring.

TABLE 12-8 SIMS Monitoring Methods and Example Thresholds

Resource	monitoring method	Threshold
IMTA queue size[1]	`immonitor-queue`	500 messages
IMTA HELD messages[2]	`immonitor-queue`	1 messages
POP, IMAP, SMTP, LDAP connect time	`immonitor-access`	5 seconds
# IMAP, POP connections[3]	`immonitor-system`	200
virtual memory	`immonitor-system`	60%
disk space: message store directory	`immonitor-system`	75%
disk space: imta channel queue directory	`immonitor-system`	50%

[1] **IMTA queue size** - This threshold will depend on the function of the IMTA. If the IMTA is responsible for routing outbound messages into the Internet, 500 is too low. 1000-2000 messages in the mail queue due to DNS problems or remote IMTA problems that are beyond the control of the local ISP are not uncommon. This number will also likely vary based on size of the ISP. If you have more customers, the chances that a mail to an address that is having problems will increase.

For internal SMTP routers, or IMTA's whose only function it is to deliver to the local message store, 500 would be too high. Except for a broadcast delivery, if the queue gets to 500 on this type of IMTA there is a problem that needs to be diagnosed.

[2]**IMTA HELD messages** - Although any number of messages may be held in the .HELD file, you should investigate even a single message caught in this file.

[3]**Number of IMAP, POP connections** - The IMAP and POP are going to be different since IMAP is a persistent connection and higher than POP.

An alternative approach to these thresholds would be to run the monitoring commands at a time of day when the service is heavily loaded, and over a period of an hour, measure the values of these resources every 5 minutes. You can then set thresholds to the highest value plus 10%.

It is likely that you will need to tune these thresholds. You can tell if they are set too low, because the thresholds will be frequently exceeded even though the service is performing satisfactorily. On the other hand, of the service fails and you were not notified in advance, the threshold may be set too high. For example if you set the disk space threshold for the message store to 95% you might not be notified in time before the disk space is exhausted.

SIMS Monitoring Examples

The monitoring utilities take snapshots of the status of the SIMS components. To provide ongoing coverage we recommend that the utilities be run periodically using a facility such as cron(1M).

The monitoring utilities use a threshold based alerting system. The administrator needs to set some threshold values and take some corrective action when they are exceeded.

For example, if the sizes of any of the IMTA queues are unusually large or there are a large number of messages in the .HELD queue, this can indicate message delivery or addressing problems. The monitoring utilities can be configured to automatically detect these scenarios and send alerts.

Scenario 1: SIMS and LDAP Server Configured on a Single Machine

In this case the various SIMS components (IMTA, message access and store, directory server, admin server) are installed on the same system. So all the monitoring utilities are scheduled to run on a single system. Also let us assume that inetmail (the SIMS Postmaster) is the user to be notified when any threshold is exceeded. Note that in this example the administrator has set up a special account named 'test_user' with a password of 'passwd' for the purposes of monitoring.

Monitored Value	Threshold
IMTA queue size	500 messages
HELD messages	100 messages
Message store size	2 gigabytes
"/" directory size	200 megabytes
SMTP connections	2000
LDAP response time	5 minutes
Mail sending time	2 minutes
POP/IMAP retrieval time	5 minutes
Schedule interval (cron)	30 minutes
Total round-trip time	5 minutes

Scenario 1 Commands:

The alert mechanism sends e-mail alerts to inetmail and to all SIMS administrators, so if the SIMS server is having mail delivery problems the alerts may not be received. Use the -A option to specify an alternate SMTP server for the alert delivery channel. For optimal monitoring, schedule the utilities to run at an interval of 30 minutes (see the crontab(1) man page). Assuming that /opt/SUNWmail/sbin is in the PATH, the corresponding crontab entries for monitoring utilities using the thresholds listed above are as follows:

- To alert inetmail when the IMTA queue size exceeds 500 messages or when the number of HELD messages exceeds 100:

```
30 * * * * immonitor queue -s 500 -H 100 -r inetmail > /dev/
null 2>&1
```

- To alert inetmail when utilization of /var/opt/SUNWmail/ims exceeds 2 gigabytes or when the utilization of "/" exceeds 200 Megabytes OR when the number of established SMTP connections exceeds 2000. The back slash (\) before the "%" is required since "%" is a keyword for crontab.

```
30 * * * * immonitor system -f /var/opt/SUNWmail/ims=2g -f /
=200m -m 90\% -p smtp=2000 -r inetmail > /dev/null 2>&1
```

- Alerts inetmail when the LDAP response time exceeds 5 minutes OR when mail sending time exceeds 2 minutes or when the mail retrieval time with POP/IMAP exceeds 5 minutes OR when the total round-trip time exceeds 5 minutes, use:

```
30 * * * * immonitor access -u test_user -w passwd -L
localhost:=300 -S localhost:=120 -I localhost:=300 -P
localhost:=300 -D 300 -r inetmail > /dev/null 2>&1
```

Scenario 2: The SIMS and LDAP Server on Different Machines

In this scenario a pure proxy server (proxy-svr) acts as a proxy for IMAP and POP requests but not SMTP. The back-end server (msma-svr) contains the message store and supports SMTP in addition to IMAP and POP protocols. Finally a dedicated server (dir-svr) provides directory services. For additional information on proxy servers, see Appendix A, "Configuring SIMS as a Proxy Message Access Server.

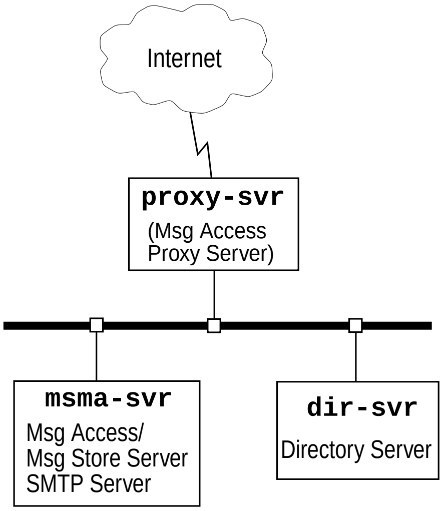


FIGURE 12-1 Monitoring Scenario 2 Environment.

Since each server isn't running the full set of SIMS services, we need to tailor the monitoring configuration on each server. In this case the services we need to monitor in the various systems are:

1. `proxy-svr:` IMAP/POP access and response time, resource utilization (cpu, disk).
2. `msma-svr:` IMAP/POP/SMTP access and response time, message round-trip delivery time, message store capacity and cpu utilization.
3. `dir-svr:` LDAP access and response time, directory capacity and CPU utilization.

We will assume the threshold values listed in the table below. As in the previous example, the alert mechanism sends e-mail alerts to `inetmail` and to all SIMS administrators, so if the SIMS server is having mail delivery problems the alerts may not be received. Use the `-A` option to specify an alternate SMTP server for the alert delivery channel. For optimal monitoring, schedule the utilities to run at an interval of 30 minutes (see the `crontab(1)`).

Thresholds and **`crontab`** *entries for* **`proxy-svr`**

Monitored Value	**Threshold**
1) IMAP: login, select inbox, close time	120 seconds
2) POP: login, stat inbox, quit time	150 seconds
3) Number of IMAP connections	500
4) Number of POP connections	250
5) Solaris: virtual memory usage	90%
6) Solaris: /var/opt used capacity	2 gigabytes

- The access times for IMAP and POP (items 1 and 2) can be checked with a single command:

  ```
  30 * * * * immonitor access -u test_user -w passwd -I proxy-
  svr:=120 -P proxy-svr:=150 -r inetmail > /dev/null 2>&1
  ```

- The number of established IMAP and POP connections (items 3 and 4) can be checked with the command:

  ```
  40 * * * * immonitor system -p IMAP=500 -p POP3=250 -r
  inetmail > /dev/null 2>&1
  ```

- Virtual memory usage (5) and the utilization of the `/var/opt` partition (6) can be measured with the following entry:

  ```
  0 * * * * immonitor system -f /var/opt=2g -m 20g -m 90\‰ -r
  inetmail > /dev/null 2>&1
  ```

Thresholds and **`crontab`** *entries for* **`msma-svr`**

Monitored Value	Threshold
1) SMTP send message tim	60 seconds
2) IMAP login, select inbox, delete time	90 seconds
3) POP login, retrieve message, close time	120 seconds
4) Number of IMAP connections	500
5) Number of POP connections	250
6) Number of SMTP connections	100
7) Message store size	2 gigabytes
8) Solaris: virtual memory usage	90%

`crontab` entries: The message delivery time comprises the sum of the times to deliver a message using SMTP and then retrieve the message using IMAP or POP. So, items (2) and (3) above are measured in conjunction with the SMTP message send time (1).

- SMTP / IMAP:

```
20 * * * * immonitor access -u test_user -w passwd -S msma-
svr:=60 -I msma-svr:=90 -k "Testing" -r inetmail > /dev/null
2>&1
```

- SMTP / POP:

```
40 * * * * immonitor access -u test_user -w passwd -S msma-
svr:=60 -P msma-svr:=120 -k "Testing" -r inetmail > /dev/null
2>&1
```

- If the IMAP or POP threshold is exceeded, messages sent using the -S option will not be deleted, so it is necessary to delete these messages periodically using another crontab entry:

```
0 * * * * immonitor access -u test_user -w passwd -I msma-
svr:=600 -z -k "Testing" > /dev/null 2>&1
```

- Established connections for POP, IMAP and SMTP can be checked with one command:

```
10 * * * * immonitor system -p POP3=200 -p IMAP=500 -p
SMTP=100 -r inetmail > /dev/null 2>&1
```

- Virtual memory usage and the size of the message store (/var/opt/SUNWmail/ims) can be measured with the following crontab entry:

```
10 * * * * immonitor system -f /var/opt/SUNWmail/ims=2g -m
90\‰ -r inetmail > /dev/null 2>&1
```

Thresholds and **`crontab`** *entries for* **`dir-svr`**

Monitored Value	Threshold
1) LDAP bind, search time	10 seconds
2) Directory size	200 megabytes
3) Solaris: virtual memory usage	90%

- LDAP:

  ```
  20 * * * * immonitor access -u test_user -L dir-svr:=10 -r
  inetmail > /dev/null 2>&1
  ```

- Virtual memory usage (3) and the size of the directory (2) (`/var/opt/SUNWconn/ldap`) can be measured with the following `crontab` entry:

  ```
  10 * * * * immonitor system -f /var/opt/SUNWconn/ldap=200m -
  m 90\‰  -r inetmail > /dev/null 2>&1
  ```

SNMP Monitoring

The Sun Directory Service is SNMP enabled. It supports the X.500 Directory Monitoring MIB (rfc1567). It can therefore be monitored by any SNMP enabled management tool. Refer to Netscape Directory Service documentation for information on Netscape SNMP support.

To enable SNMP monitoring of the Sun Directory Service you should first enable the SNMP agent `dsnmpserv(1m)`. The following describes how to enable this service:

1. **Configure the SNMP configuration file /etc/opt/SUNWconn/ldap/current/dsnmpserv.conf by running the following command:**

   ```
   /opt/SUNWconn/sbin/dsnmpcfg
   ```

2. **Start the agent:**

   ```
   /etc/init.d/init.dnsmpserv start
   ```

CHAPTER **13**

SIMS Troubleshooting

Topic/Task	Description	Page
Troubleshooting the Admin Console	- Netscape Applet Loading Problem - Admin Server Crash Recovery - Preventing the “Warning Applet” Banner - Forgetting the Admin Password	270
Troubleshooting the Administration Server	- Java Exceptions When Administration Server Starts - java.lang.OutOfMemoryError While Administration Services Starts - Admin Console Displays “Failed to locate SIMS Administration Server”	271
Troubleshooting the Message Store	- User Not Able to Access INBOX - Problems Turning Message Store Quota Enforcement Off and On - Message Purge Failure - User Can’t Perform Internationalized String Search on Mail Messages	274
Troubleshooting the IMTA	- SMTP Connection Aborted - Message Queue Problems - Logging and Tracking Messages in the IMTA - Address Unknown to IMTA - Multiple Reprocess Jobs Generated - IMTA Error Messages	278
Troubleshooting the Directory Service	- Diagnosing SIMS Problems Caused by Improper Directory Entries - Re-generating the Sun Directory Service Directory Index	295
Crash Recovery	- SIMS Crash Recovery - Message Store Crash Recovery - Admin Console Crash Recovery	297
Error Messages	Go to Appendix D, “Error Messages.”	329

Troubleshooting the Admin Console

Netscape Applet Loading Problem

This indicates that the Netscape Navigator does not reload the applets properly. If you are in any component page, and you want to reload the page, use the browser back arrow to go back to the Console main page and reselect the component icon. If you are in the Admin Console main page, logout, and re-login again. If none of this works, you may need to stop and restart the browser, and reconnect to the SIMS admin server again.

If applet appears to not be loading. You may need to move the mouse or select some menu buttons from the browser to activate the process.

Preventing the “Warning Applet” Banner

When accessing the Admin Console using a Netscape browser, you may see a “Warning Applet” banner in all dialogs. To prevent this banner from appearing, first close all browsers and do the following:

If you are using the Netscape browser (4.X and above), you **MUST** add the following line must be in the `preferences.js` file in the `.netscape` directory for the Admin Console to run correctly:

```
user_pref("signed.applets.codebase_principal_support",true);
```

Note – It is always a good idea to make these changes as some Admin Console functions won’t work otherwise.

Forgetting the Admin Password

If you forget any SIMS Administrator password, you can use the `admin-modify-user` utility (you'll need to provide the `binddn` and `password` of another administrator) to change the password. If you have only one SIMS administrator and you forget this password, you'll need to contact your Sun Microsystems support person.

Troubleshooting the Administration Server

To Restart the Admin Server

1. **On rare occasions the Admin Server will crash and you may need to restart it using the following command:**

```
# /opt/SUNWmail/sbin/adm.server stop
# /opt/SUNWmail/sbin/adm.server start
```

Java Exceptions When Administration Server Starts

Exceptions 1: If the following Java exception is thrown when the administration server is starting:

```
java.rmi.server.ExportException: Port already in use: 1099;
nested exception is:
    java.net.BindException: Address already in use
    at java.lang.Throwable.<init>(Compiled Code)
    at java.lang.Exception.<init>(Compiled Code)
    at java.io.IOException.<init>(Compiled Code)
```

```
...
```

This could be caused by one of two possible reasons:

1. Some other JAVA application is using RMI, and the RMI default port was used.
2. You stopped, then started the admin server too quickly and the RMI registry did not completely end the process. The procedure to handle these two situation is:

- Run `/opt/SUNWmail/admin/sbin`, type `adm.server stop`
- Wait 30 seconds and start the admin server again: type adm.server start.
- If you still see the Exception, go to /opt/SUNWmail/html, edit the simsadmin_port.html file, and change the number 1099 to another port number.
- Stop and start the admin server.

Exceptions 2: Another JAVA exception thrown when the admin server is starting:

```
AdminServerImpl err: Server RemoteException; nested exception is:
          java.rmi.AccessException: Registry.rebind
          java.rmi.ServerException: Server RemoteException;
          nested exception is:
          java.rmi.AccessException: Registry.rebind
         AdminServerImpl fails to register
```

This may be caused by the DNS setup. View the `/etc/nsswitch.conf` file. Is the format configured as "`hosts: dns files`" or "`hosts: files dns`?"

If a hostname is not understood by the DNS table, then the RMI will have problems. If this occurs, change the order of the host to "`files dns`" then the admin server can be started.

java.lang.OutOfMemoryError While Administration Services Starts

If the Java program runs out of memory you will receive the following error:

```
# java.lang.OutOfMemoryError: /var/opt/SUNWmail/ims/user/080
   at java.io.File.list(Compiled Code)
   at COM.Sun.sunsoft.sims.admin.ms.MSUserFolderInfo.<init>(Compiled Code)
   at COM.Sun.sunsoft.sims.admin.ms.MSManagedObjectImpl.<init>(Compile Code)
  at COM.Sun.sunsoft.sims.admin.console.RegistryLoader.loadFiles(Compiled Code)
   at COM.Sun.sunsoft.sims.admin.console.RegistryLoader.<init>(Compiled Code)
   at COM.Sun.sunsoft.sims.admin.console.AdminServerImpl.init(Compiled Code)
   at COM.Sun.sunsoft.sims.admin.console.AdminServerImpl.main(Compiled Code)
```

To fix the problem go into `/opt/SUNWmail/sbin/adm.server` and change

```
$JAVA -Ddirectoryhost=${DIRECTORYHOST} \
```

to

```
$JAVA -oss2m -ms32m -mx64m -Ddirectoryhost=${DIRECTORYHOST} \
```

and then stop and start the admin server

Admin Console Displays “Failed to locate SIMS Administration Server”

Your admin server did not fully start up because of a component configuration error. Start the admin server in debug mode:

```
/opt/SUNWmail/admin/sbin/adm.server stop
/opt/SUNWmail/admin/sbin/adm.server -d All -l 6 start
```

If there are JAVA exceptions displayed, it means the admin server did not come up. Write down the exception information and send it to your SIMS support personal for more help.

If there aren’t any JAVA exceptions, then it could be a browser connection time-out. Usually, an http proxy is set in the browser’s preferences window. JAVA applets are downloaded from the server machine through the proxy server, and then to the client machine. This could take a long time depending on how the network is setup. Try removing the http proxy setting in your browser environment, and then try to reload the SIMS page again.

Troubleshooting the Message Store

User Not Able to Access INBOX

If an administrator created a new `/var/mail` account on SIMS using the Admin Console, and she forgot to create a UNIX account, the user will not be able to read the INBOX. The following error message will appear:

```
Unknown uid: <username>
```

The solution is to create the UNIX login account and the home directory:

1. **All `/var/mail` store users must have a shell account and HOME directory setting.**

2. **Create the UNIX shell account using the desired operating system tools (for example, `admintool`).**

3. **Using the Admin Console set the Home Directory field.**

Verifying Password and Login

If a user cannot log in to his mailbox, you can determine if the correct login and password is being used by doing the following:

1. **Obtain the password and login which the POP/IMAP user is using.**

   This corresponds to the `userPassword` and `uid` attributes in the LDAP record for that person. `userPassword` is stored as an encrypted string (unless APOP is used, in which case it might be clear text). If you dump the record it will display as encrypted just as it would in the `/etc/shadow` file. Note that the password will only display if you can bind as that user successfully, or if you bind as the administrator distinguished name.

2. **Use the** `uid` **to get the distinguished name for that person's record.**

   The example below is for an entry on an LDAP server "fork", using a search-base appropriate to bridge.

   ```
   % /opt/SUNWconn/bin/ldapsearch -h fork -L -b "dc=bridge,\
   dc=com,o=internet" uid=rja dn
   ```

   ```
   dn: cn=Rob Albert (rja),ou=People,dc=bridge,dc=com,o=internet
   ```

3. **Using the value of the distinguished name retrieved in the previous step (but just the value, not the attribute tag "**`dn:`**") try to bind to the directory as that user, using the password (in cleartext) that the user is trying to login as:**

   Example 1 (bad password, good DN):

   ```
   % /opt/SUNWconn/bin/ldapsearch -h fork -L -b "o=internet" \
    -D "cn=Rob Albert (rja),ou=People,dc=bridge,dc=com,o=internet"\
   -w badpass uid=rja dn
   ```

   ```
   ldap_bind: Invalid credentials
   ```

   Example 2 (good password, good DN):

   ```
   % /opt/SUNWconn/bin/ldapsearch -h thestork -L -b "o=internet" \
   -D "cn=Rob Albert (rja),ou=People,dc=bridge,dc=com,o=internet" -w\
   goodpass uid=rja dn
   ```

   ```
   dn: cn=Rob Albert (rja),ou=People,dc=bridge,dc=com,o=internet
   ```

   Example 3 (good password, bad DN):

   ```
   % /opt/SUNWconn/bin/ldapsearch -h thestork -L -b "o=internet" \
   -D "cn=Rob Albert (rja),ou=People,dc=bridge,dc=com,o=internet" -w \
   goodpass uid=rja dn
   ```

   ```
   ldap_bind: No such object
   ldap_bind: matched: ou=People,dc=bridge,dc=com,o=internet
   ```

   Example 4 (good password, good DN, but the wrong "uid=" value):

   ```
   % /opt/SUNWconn/bin/ldapsearch -h thestork -L -b "o=internet" \
   -D "cn=Rob Albert (rja),ou=People,dc=bridge,dc=com,o=internet" -w \
   goodpass uid=fred
   ```

   ```
   dn: CN=Frederic Herrmann
   (fred),ou=People,dc=bridge,dc=com,o=internet
   ```

   In the above examples you first bind anonymously to the directory to get the distinguished name of whom you want to bind as. Then you bind as that person, using their distinguished name and password. If you cannot bind as the user, then either their password or their distinguished name is wrong. If you *can* bind as the user, but they still can't log in, then either their LDAP record is damaged (you can verify this by comparing their record to a known undamaged record), or possibly the DITs are misconfigured (they may be confusing where the user data is to be looked up or the `ims-basedn` value in `/etc/opt/SUNWmail/ims/ims.cnf` does not match the DIT structure). This is not a complete list, but it covers the most common misconfigurations).

Problems Turning Message Store Quota Enforcement Off and On

If for some reason you turn the message store quota enforcement off, modify a user's quota, and then turn message store quota enforcement back on again, you should shut down SIMS. If you don't, it's possible that for a short period incoming mail to the modified user will be temporarily not delivered and returned to the sender. We absolutely recommend that you NOT turn the quota enforcement off to modify a user's quota, but in the very rare and unusual circumstance that you do, use the following procedure:

1. Shut down SIMS.

2. Do whatever work you need to do with quota turned off.

3. Turn the quota back on.

4. Run `iminitquota -a`.

5. Restart SIMS.

Here's an example of how a mail store full situation could occur, even though the mail store is not full:

A user, *Galaxion*, has a user quota of 20 Mbytes and is currently using 15 Mbytes.

The message store quota enforcement is turned off, and while it is turned off, three things happen:

1) Galaxion's quota is reduced to 10 Mbytes.

2) Galaxion deletes a large amount of mail and reduces her mail store usage to 7 Mbytes.

3) An incremental directory synchronization occurs.

When quota enforcement is turned back on, `iminitquota -a` must be run to tally up mail storage usage. As soon as an incremental directory synchronization occurs, the system starts to enforce the new quota—in this case, 10 Mbytes.

However, the system reads the old mail store usage value of 15 Mbytes, until `iminitquota -a` is finished running. For 10,000 users, this might take 30 minutes. For that 30-minute period, the new quota of 10 Mbytes might be used, but the old mail store usage value of 15 Mbytes is read. This causes the enforcement to stop accepting new mail.

Message Purge Failure

The `impurge` command fails if the file system is full. You will see the following error message in the `syslog` file:

```
Jul 11 12:52:27 mcm-charmed SUNWmail.ims.impurge[17436]: PURGE
erro: Cannot create expungedir tmp file
Jul 11 12:52:27 mcm-charmed SUNWmail.ims.impurge[17436]: PURGE
erro: Cannot create ADM expungedir tmp file
```

To recover from this scenario, one can use the `impurge -f dirname` and follow the sequence of steps below:

1. Create a clean file system with sufficient disk space, (this is twice as much space as the largest amount of data residing in the daily message store bucket, that is, an amount larger than the message data stored on the system’s busiest day).
2. Mount the clean file system with a name of your choice, for example, `/backup`
3. Run the impurge command as `impurge -f /backup.` This will allow the purge command to complete the purging operations.
4. Upon completion, the `/backup` directory will be empty and the messages will be purged.

If the file system is 100% full, you must run the `impurge -f` command as root.

In case of a system crash during the middle of a purging operation, you should make sure the `/backup` file system is mounted before running the command again.

User Can’t Perform Internationalized String Search on Mail Messages

SIMS supports internationalized string searches in mail messages using any major character set. Search strings are no longer limited to ASCII/English.

Some mail clients, however, perform searches locally. That is, they use client code to perform searches. This client code might or might not support an internationalized search. To perform an internationalized search using the SIMS search code, mail clients must send an `IMAP SEARCH` command to the server.

If a mail user cannot do an internationalized search, make sure that the particular mail client used sends an `IMAP SEARCH` command to the server.

Troubleshooting the IMTA

Standard IMTA Troubleshooting Procedures

In tracking down problems with the IMTA you should do the following:

- Determine whether the problem occurs before or after a message is entered into the message queue
- Determine whether messages were never accepted because of configuration problems or environmental problems (e.g., disk space or quota problems) or the absence of IMTA servers such as the Dispatcher and its services that can prevent the IMTA from accepting messages

- Determine if network connectivity or routing problems could mean that the messages are stuck or mis-routed on a remote system.

If messages do not get placed in a queue directory at all, or get put into the wrong queue directory, you probably have a configuration problem.

To track an errant mail message, you can start by examining each step of the process for errors. The subsections below discuss investigating these processing steps.

Check the IMTA Configuration

Use the `imta test -rewrite` utility (see the `imta-test-rewrite` man page), to test the response of your configuration to addresses. Certain basic sorts of problems in the IMTA configuration, such as clear syntax errors in the IMTA configuration, will cause the utility to issue an error message. Otherwise, the utility will show address rewritings that will be applied as well as the channel to which messages would ultimately be queued. If the output is not what you expect you may need to modify your configuration.

Check Message Queue Directories

Check whether messages are present under the IMTA message queue directory, `/var/opt/SUNWmail/imta/queue/`. Shell commands such as `imta qm` utility's directory command may be used to check for the presence of expected message files under the IMTA message queue directory.

If the `imta test -rewrite` output looks correct, check that messages are actually being placed in the IMTA message queue subdirectories. If not, you may have a problem with file space on that disk.

Check the Ownership of Critical Files

You should have an administrator (inetmail by default) account, created when you installed the IMTA. The directories `/var/opt/SUNWmail/imta/queue/`, `/var/opt/SUNWmail/imta/log`, and `/var/opt/SUNWmail/imta/queue_cache`, and all subdirectories and files under them should be owned by the inetmail account. If the protection and ownership are not correct for the queue cache database, messages may not be entered into the queue cache, and the queue cache will not be synchronized with the directory. Commands such as the following may be used to check the protection and ownership of these directories:

```
# ls -l -p -d /var/opt/SUNWmail/imta/queue
drwx------ 6 inetmail   bin     512  Feb  7 09:32 /var/opt/SUNWmail/imta/queue/
# ls -l -p -d /var/opt/SUNWmail/imta/log
drwx------ 2 inetmail   bin    1536 Mar 10 20:00 /var/opt/SUNWmail/imta/log/
# ls -l -p -d /var/opt/SUNWmail/imta/queue_cache
drwx------ 2 inetmail   bin   512  Mar 10 15:03 /var/opt/SUNWmail/imta/
queue_cache/
```

Then check that any files and subdirectories of **`/var/opt/SUNWmail/imta/queue`** and **`/var/opt/SUNWmail/imta/log`** are owned by the IMTA account using commands such as:

```
# ls -l -p -R /var/opt/SUNWmail/imta/queue
# ls -l -p -R /var/opt/SUNWmail/imta/log
```

Checking that the Job Controller and Dispatcher are Present

The IMTA Job Controller handles the execution of the IMTA processing jobs, including most outgoing (master) channel jobs.

Some IMTA channels, such as the IMTA's multi-threaded SMTP channels, include resident server processes that process incoming messages---such servers handle the slave (incoming) direction for the channel.

The IMTA Dispatcher handles the creation of such IMTA servers. Dispatcher configuration options control whether such servers are available at all, and if available, how many such servers are created and when, and how many connections each server can handle. The Dispatcher always keeps at least one SMTP server process resident.

The command

```
# imta process
```

can be used to check that the IMTA Job Controller and IMTA Service Dispatcher are present, and to see if there are IMTA servers and processing jobs running. Under idle conditions the command should result in `job_controller`, `dispatcher` and `tcp_smtp_server`.

Check Processing Log Files

If the IMTA processing jobs run properly but the message stays in the message queue directory, you can examine the log files to see what is happening. All log files are created in the directory `/var/opt/SUNWmail/imta/log`. Log file name formats for various IMTA processing jobs are shown below.

TABLE 13-1 IMTA log files on UNIX

File name	Log file contains
`channel_master.log-uniqueid`	Output of master program (usually client) for channel
`channel_slave.log-uniqueid`	Output of slave program (usually server) for channel
`dispatcher.log-uniqueid`	Dispatcher logging, if the Dispatcher DEBUG option has been set
`job_controller.log-uniqueid`	Job controller logging, if the Job Controller option DEBUG=1 has been set
`server-name_server.log-uniqueid`	Logging for the server server-name
`server-name_thread.log-uniqueid`	Per thread errors for server-name
`post.log- uniqueid`	Log output for the periodic IMTA delivery job
`return.log- uniqueid`	Log output for the periodic IMTA message bouncer job

Channel log files are not created unless an error occurs or unless debugging output is enabled for the channel with the `master_debug` channel keyword or `slave_debug` channel keyword.

Each new log file is created with a unique id to avoid overwriting an earlier log written by the same channel. You can use the `imta find` utility to aid in finding the desired “version” of a log file. You can purge back older log files using the `imta purge` command.

Running a Channel Program Manually

While diagnosing an IMTA delivery problem it may be useful to run an IMTA delivery job by hand, particularly after enabling debugging output for one or more channels. The command

```
# imta submit channel-name
```

will notify the IMTA Job Controller to run the channel. If debugging is enabled for the channel in question, `imta submit` will create a log file in `/var/opt/SUNWmail/imta/log`. See “Logging Messages Passing Through the IMTA” on page 254.

The command

```
# imta run channel-name
```

will perform outbound delivery for the channel channel-name under the currently active process, with output directed to your terminal. This may be more convenient than submitting a job, particularly if you suspect problems with job submission itself.

▼ To Start and Stop Individual Channels

This section tells how to stop message enqueueing and dequeueing so that message queue problems may be more easily diagnosed and debugged. Freezing the message queue allows you to examine queued messages to determine the existence of loops, spam attacks, or mail bombs.

1. To stop outbound processing (dequeueing) for a specific channel, edit the channel's channel block in `imta.cnf` and add the `slave` channel keyword. Then run `imta cnbuild`.

   To resume processing, remove the keyword and run `imta restart job.controller` as root.

2. To stop inbound processing (enqueuing to a channel) for a specific channel, without bouncing messages, redirect messages destined to this channel to the hold channel by replacing the channel's routing system with `hold-daemon` in the rewrite rules. Then restart the IMTA by executing `imta restart`. Messages are enqueued to the hold channel.

   To resume inbound processing, change the routing system back to its original setting and restart the IMTA. Then run

   ```
   /opt/SUNWmail/imta/sbin/hold_master -u "*" -d "*"
   ```

   Note that you should not be using the hold channel for any other purpose (such as moving a user) while you are performing this process.

3. To stop inbound processing (enqueuing to a channel) while returning temporary SMTP errors to client hosts, add the following access rule in the SEND_ACCESS mapping table in the IMTA mappings file:

   ```
   SEND_ACCESS
   
   *|*|your_channel|*   $X4.2.1|$Ndestination$ channel$
   temporarily$ disabled
   ```

Changes to Configuration Files or IMTA Databases Do Not Take Effect

If changes to your configuration, mapping, conversion, security, option, or alias files or to IMTA databases do not seem to be taking effect, check to see if you have restarted your mail user agent session, and that you have restarted the IMTA.

IMTA Sends Outgoing Mail But Does Not Receive Incoming Mail

Most IMTA channels depend upon a slave, or server, channel program to receive incoming messages. For some transports supported by the IMTA, in particular TCP/IP and UUCP, you need to make sure that the transport activates the IMTA slave program rather than its standard server. Replacing the native sendmail SMTP server with the IMTA SMTP server is performed as a part of installation task.

For the multi-threaded SMTP server, the startup of the SMTP server is controlled via the IMTA Dispatcher. The IMTA Dispatcher controls the starting up of an SMTP server or servers, according to your Dispatcher configuration. If the Dispatcher is configured to use a `MIN_PROCS` value greater than or equal to one for the SMTP service, then there should always be at least one SMTP server process running (and potentially more, according to the `MAX_PROCS` value for the SMTP service). The `imta process` command may be used to check for the presence of SMTP server processes. Use `dispatcher_stats_tty` to check SMTP processes connection.

Time Outs on Incoming SMTP Connections

Time outs on incoming SMTP connections are most often related to system resources and the allocation thereof.

Check how many simultaneous incoming SMTP connections you allow. This is controlled by the `MAX_PROCS` and `MAX_CONNECTIONS` Dispatcher settings for the SMTP service; the number of simultaneous connections allowed is `MAX_PROCS*MAX_CONNECTIONS`. If you can afford the system resources, consider raising this number if it is too low for your usage.

Try putting the slave_debug keyword on the channels handling incoming SMTP over TCP/IP mail, usually `tcp_local`. Then take a look at the resulting `tcp_local_slave.log-uniqueid` files, and try to spot any particular characteristics of the messages that time out. For instance, if incoming messages with large numbers of recipients are timing out, consider using the `expandlimit` keyword on the channel.

Of course, if your system is extremely overloaded and overextended, time outs will be difficult to avoid entirely.

Message Queue Growing Because a Recipient Address is Slow Accepting Email

Sometimes, it becomes necessary to separate the messages going to one or more specific email sites because the remote SMTP servers at those sites are slow or not responding and it holds up all the outgoing mail. This can be done by creating a new channel, similar to the external SMTP channel and a new processing queue, associated with it, for all mails going to those domains.

For example, if you want to separate out all mail going to `slow.com`, first you create a new channel and it's rewrite rules. That is, in the IMTA configuration file, `/etc/opt/SUNWmail/imta/imta.cnf` add lines similar to the following:

```
!Rewrite rules
..........
! tcp_slow
.slow.com $E$U%$H.slow.com@tcp_slow-daemon
.slow $U%$H.slow.com@tcp_slow-daemon
!
...........
!Channel definitions
...........

!
! tcp_slow
tcp_slow queue slow_queue smtp single_sys copywarnpost
copysendpost postheadonly
switchchannel subdirs 20 immnonurgent logging notices 1 2 4 7
remotehost inner
tcp_slow-daemon mailserver.acme.com

!
..........

 Note the usage of the queue keyword to separate the message
processing queue.
```

```
Also edit the job controller configuration file, /etc/opt/
SUNWmail/imta/job_controller.cnf
and add the following lines, in the queue definitions section :

...........
!
[QUEUE=SLOW_QUEUE]
job_limit=10
capacity=200
!
..............
```

SMTP Connection Aborted

If the SMTP connection aborts, check whether the IMTA is running (SMTP server included):

```
% imta process
```

The result should list the three following processes:

```
job_controller
dispatcher
tcp_smtp_server
```

Restart the IMTA if it is not running.

If the IMTA continues to abort, look at the `tcp_smtp_server` log files to determine the problem.

```
/var/opt/SUNWmail/imta/log
```

To debug the IMTA problem, set `debug=1` in `/etc/opt/SUNWmail/imta/dispatcher.cnf`. Also enable the diagnostic output for the slave program in the internet channel. (From the IMTA Property Book double-click the relevant SMTP channel and go to the *Diagnostics Output Section*. Check the box for *Enable diagnostic output for slave program*.

Try to start the IMTA again, and look at the debug output in the `tcp_smtp_server` log files at `/var/opt/SUNWmail/imta/log/tcp_local_slave*`.

Sent Message Can’t Find Server Name

If DNS is not working, the administration server will display the following warning message in a console window:

```
***Can’t find server name for address <ip_address>: No response
from server. ***Default servers are not available
```

In addition, a Java exception stack will be displayed, and users will not be able to send mail until the DNS is once again operating.

The administration server does not itself depend on the DNS server—it can continue to operate and an Admin Console can connect to it. But the DNS server needs to be returned to normal operation before mail can be sent.

Message Queue Problems

Undeliverable messages are probably either not being dequeued from the IMTA, being saved in `.HELD` file because it is looping between another server or channel, or stuck at another server. This section describes various message queue problems.

Unjamming a Message Queue

If the IMTA stops processing messages in a queue, enter the following command as `root` for the queue that appears jammed:

```
# /opt/SUNWmail/sbin/imta run <channel name>
```

where `<channel name>` is specified in `imta.cnf`

Message Not Being Dequeued

Errors encountered during TCP/IP delivery are quite often transient in nature and the IMTA will generally retain messages when problems are encountered and retry them periodically. It is quite normal on very large networks to experience periodic outages to certain hosts while other host connections work fine. You can examine the log files for errors relating to delivery attempts. You may see error messages such as “Fatal error from smtp_open.” Such errors are not uncommon and are usually associated with a transient network problem. Your TCP/IP package may contain tools such as ping, traceroute, and nslookup to aid in debugging TCP/IP network problems.

The example below shows the steps you might use to see why a message is sitting in the queue awaiting delivery to xtel.co.uk. The basic idea is to duplicate the steps the IMTA uses to deliver SMTP mail on TCP/IP.

```
% nslookup -query=mx xtel.co.uk     (1)
Server:  LOCALHOST
Address:  127.0.0.1

Non-authoritative answer:
XTEL.CO.UK      preference = 10, mail exchanger = nsfnet-relay.ac.uk (2)

% /usr/sbin/ping nsfnet-relay.ac.uk      (3)
PING NSFNET-RELAY.AC.UK (128.86.8.6): 56 data bytes
64 bytes from 128.86.8.6: icmp_seq=0 time=490 ms
CANCEL

% telnet nsfnet-relay.ac.uk 25       (4)
Trying... [128.86.8.6]
telnet: Unable to connect to remote host: Connection refused
```

1. First use the NSLOOKUP utility to see what MX records, if any, exist for this host. If no MX records exist, then you should try connecting directly to the host. If MX records do exist, then you must test by connecting to the designated MX relays since the IMTA is required to honor MX information preferentially.

2. In this example, the Domain Name Service returned the name of the designated MX relay for xtel.co.uk. This is the host that the IMTA will actually connect to. If more than one MX relay is listed, the IMTA would try each in succession.

3. A simple way to test connectivity to the host is with a PING utility. If no response is received then you have a network routing or configuration problem. If the problem is on some router over which you have no control, there is not anything you can do except to wait until it is fixed.

4. If you do have connectivity to the remote host, the next step is to see if it is accepting inbound SMTP connections by using TELNET to the SMTP server port, port 25. If you use TELNET without specifying the port, you may merely discover that the remote host accepts normal TELNET connections. This by no means indicates that it accepts SMTP connections: many systems may accept regular TELNET connections but refuse SMTP connections or vice versa. Thus, you should always do your testing against the SMTP port.

   In this example, the remote host is currently refusing connections to the SMTP port. This is undoubtedly why the IMTA fails to deliver the message. The connection may be refused due to a misconfiguration of the remote host or some sort of resource exhaustion, again, on the remote host. There is absolutely nothing you can do locally to solve the problem. Typically, you should just let the IMTA continue to retry the message.

If you are running on a TCP/IP network which does not use the Domain Name Service, then you can skip steps (1) and (2) and use PING and TELNET directly to the host in question. Be careful to use precisely the host name that the IMTA would use, which can be ascertained by examination of the relevant log file from the IMTA's last attempt.

Note that if you test connectivity to a TCP/IP host and encounter no problems using interactive tests, it is quite likely that the problem has simply been resolved since the IMTA last tried delivering the message. This is not an indication of a problem with the IMTA.

IMTA Messages are Not Delivered

In addition to message transport problems, there are two other common problems which can lead to messages sitting around unprocessed in the message queues:

1. The message has a low priority. By default, the IMTA pays attention to Priority: headers in scheduling message delivery jobs: only messages of normal or urgent Priority: get an immediate delivery attempt, while messages of non-urgent Priority: wait until the next run of the IMTA periodic delivery job.

2. The queue cache database is not synchronized with the messages in the queue directories.

   Message files in the IMTA queue subdirectories which are awaiting delivery are entered into the queue cache database. When channel programs run in order to deliver messages in their queues they consult the queue cache to determine what messages to process. There are circumstances which can lead to message files in the queue that do not have a corresponding queue cache entry. For example, if the queue cache database has incorrect ownership and protection, see "Check the Ownership of Critical Files" on page 279. Channel programs will ignore queued messages which do not have a cache entry. You can use the `imta cache -view` utility to check if a particular file is in the queue cache; if it is not, then the queue cache needs to be synchronized.

   The queue cache is normally synchronized daily. If required, you can manually resynchronize the cache using the UNIX command

   ```
   # imta cache -synchronize
   ```

   Once synchronized, upon the next running of the IMTA periodic delivery job the channel programs should process all messages in their queue.

There is a more drastic step, rebuilding the queue cache database, which should only be performed as a last resort, e.g., if disk problems have corrupted your queue cache database, as it will cause loss of some information from the queue cache database. (The sort of information lost includes, but is not limited to, message creation dates, message deferral dates, message expiration dates, and the original message owner information.)

To rebuild the queue cache database, use the UNIX commands,

```
# imta cache -rebuild
# imta cache -close
# imta cache -synchronize
```

3. Channel processing programs fail to run because they cannot create their execution log file.

   Check the access permissions, disk space and quotas.

.HELD Messages

If the IMTA detects a mail loop, that is, messages bounce between servers/channels, delivery is halted and the messages are stored in a file with the suffix `.HELD` in `/var/opt/SUNWmail/imta/queue/<channel>`. (A mail loop occurs because each server/channel thinks the other is responsible for delivery to an address.)

The message is ignored by the IMTA and no further delivery is attempted. Look at the headers in the message to determine which server/channel is bouncing the message. Fix the entry as needed and run the command:

```
% imta queue -retry_delivery <channel-name>
```

Messages are Looping

If the IMTA detects that a message is looping, that message will be sidelined as a .HELD file. But certain cases can lead to message loops which the IMTA can not detect. Some of the more common cases include:

1. A postmaster address is broken.
2. Stripping of Received: headers is preventing the IMTA from detecting the message loop.
3. Incorrect handling of notification messages by other mail systems, that are generating reencapsulated messages in response to notification messages.

The first step in dealing with looping messages is to determine why the messages are looping. Useful things to look at are a copy of the problem message file while it is in the IMTA queue area, IMTA mail log entries (if you have the logging channel keyword enabled in your IMTA configuration file for the channels in question) relating to the problem message, and IMTA channel debug log files for the channels in question. Determining the From: and To: addresses for the problem message, seeing the Received: headers, and seeing the message structure (type of encapsulation of the message contents), can all help pinpoint which sort of message loop case you are encountering.

For case (1), note that mail systems such as the IMTA require that the postmaster address be a functioning address that can receive e-mail. If a message to the postmaster is looping, check that your configuration has a proper postmaster address pointing to an account that can receive messages.

For case (2), note that normal detection of message loops is based on various Received: headers. If Received: headers are being stripped---either explicitly on the IMTA system itself, or more likely on some other system such as a firewall---that interferes with proper detection of message loops. There will likely be two issues to resolve: check that no undesired stripping of Received: headers is occurring so that if a loop does occur it can be short-circuited, and check for the underlying reason why the messages were looping. Possible underlying reasons for the occurrence of the message loop in the first place include: a problem in the assignment of system names or a system not configured to recognize a variant of its own name, a DNS problem, a lack of authoritative addressing information on the system(s) in question, or a user address forwarding error.

For case (3), note that Internet standards require that notification messages (reports of messages being delivered, or messages bouncing) have an empty envelope From: address to prevent message loops. However, some mail systems do not correctly handle such notification messages; such mail systems may, when forwarding or bouncing such a notification message, insert a new envelope From: address of their own. This can then lead to message loops. The solution is to fix the mail system that is incorrectly handling the notification messages.

Received Message is Encoded

Messages sent by the IMTA are received in an encoded format. For example:

```
Date: Sun, 04 Jul 1993 11:59:56 -0700 (PDT)
From: "Wally C. Bouy" <wallyboy@bridge.com>
To: Padraic.Fanning@stream.edu
Subject: test message with 8bit data
MIME-Version: 1.0
Content-type: TEXT/PLAIN; CHARSET=ISO-8859-1
Content-transfer-encoding: QUOTED-PRINTABLE

2=00So are the Bo=F6tes Void and the Coal Sack the same?=
```

Such messages appear unencoded when read with a MIME-aware user agent such as Pine or when decoded with a decoder such as `imta decode.`

The SMTP protocol as set forth by RFC 821 only allows the transmission of ASCII characters. As ASCII is a seven-bit character set, the transmission via SMTP of eight bit characters is illegal. As a practical matter, the transmission of eight bit characters over SMTP is known to cause a variety of problems with some SMTP servers (for example, cause SMTP servers to go into compute bound loops, cause mail messages to be sent over and over again, crash SMTP servers, wreak havoc with user agents or mailboxes which cannot handle eight bit data, and so on).

Until the advent of RFC 1425 and RFC 1426, an SMTP client had only three alternatives when presented with a message containing eight bit data: return the message to the sender as undeliverable, encode the message, or send it anyhow in direct violation of RFC 821. None of these alternatives were pleasant. With the recent advent of MIME (first specified in RFCs 1521 and 1522, and updated in RFCs 2045--2049) and the SMTP extensions work (RFC 1425 and RFC 1426), there are now standard encodings which may be used to encode eight bit data using the ASCII character set and mechanisms to negotiate, between the SMTP client and server, whether or not eight bit data will be accepted as is by the server without first being encoded.

When recipients receive encoded messages such as those shown above with a MIME content type of TEXT/PLAIN, then invariably the original message contained eight-bit characters and the remote SMTP server to which the IMTA SMTP client transferred the message did not support the transfer of eight bit data. The IMTA then had to encode the message.

From: Address Missing in Notifications from the IMTA

Occasionally users or postmasters on other mail systems will complain that the IMTA is omitting the envelope From: address in messages it sends. You may be presented with a message header fragment like the one shown below

```
From    Thu Jan 13 11:50:23 1994
Received: from vulcan.ajax.com by monster.ajax.com via SMTP
     (930416.SGI/931108.SGI.ANONFTP) for xxxx id AA21154;
     Thu, 13 Jan 94 11:50:23 +1100
Date: Thu, 13 Jan 1994 11:49:26 +1000
From: IMTA Mail Server <postmaster@vulcan.ajax.com>
```

Note how in the first line there is a noticeable blank space between the From and date? This header line is often referred to as the *colonless From line* and it gives the envelope From: address for the message. That blank space indicates that the message had no envelope From: address; that is, it had what is called in the mail business a null return path. Note further that this was an automatically generated mail message as suggested by the RFC 822 From: address of postmaster@vulcan.ajax.com.

The relevant standards require that automatically generated messages such as non-delivery notifications and delivery receipts use a null return path. As mailers are supposed to bounce mail to the envelope From: address[1], this helps to prevent mail loops from occurring.

If someone complains about the missing the From: address, ask them to send you a sample offending message. Determine if it was an automatically generated message. If it was, then explain to them that if their mailer or user agent is incapable of handling null return paths then it is incompliant with RFC 821 and 1123. Refer them to Paragraph 8 of Section 3.6 and the second paragraph of the MAIL command description in Section 4.1.1 in RFC 821. Further point out that were you to change your mailer to use a non-null return path for automatically generated notifications, then you would be violating the Internet Host Requirements; specifically, you would be in violation of Section 5.3.3 of RFC 1123.

If for some reason you absolutely must generate non-null return paths in your notification messages, then you may do so with the RETURN_ENVELOPE option of the IMTA option file (see *SIMS Reference Manual*). Or to generate non-null return paths in notification messages only for a particular channel or channels, you may use the returnenvelope channel keyword (refer to the keywords section in the *SIMS Reference Manual*). Be warned: Use of either the option or the channel keyword will put you in violation of the Internet Host Requirements and, more importantly, may lead to looping mail. Looping mail will not only inconvenience you but may

[1] Some mailers will preferentially send notifications to the address specified with the non-standard Errors-to: or Warnings-to: header lines. By default, the IMTA itself sends notifications to the envelope From: address, unless configured otherwise via the USE_ERRORS_TO and USE_WARNINGS_TO IMTA options.

cause serious problems for some unfortunate site which gets into a loop with your system. Also, keep in mind that changing the IMTA's behavior so as not to cause problems for a broken mailer which cannot handle null return paths does not really fix anything: Other mailers over which you have no control will continue to send the broken mailer messages with null return paths. The only satisfactory solution in this situation is to fix the broken mailer.

Address Unknown to IMTA

If a sender sends a message to a valid address and receives a returned message with the error "User unknown," verify the address by using the `imta test -rewrite` command. Most likely the user entry in the directory is not correct. Retrieve the full directory entry for this user, and verify it. IMTA `dirsync` can also check directory entry errors. Enter the command:

```
# imta dirsync -t -F
```

If no invalid entries are reported, try running `dirsync` again with the `-v` switch, and look at the newest `/var/opt/SUNWmail/log/dirsync.trc-*` for more information.

Once you've fixed the directory user info, you may run `dirsync` again, or wait until the periodic incremental `dirsync` runs. Run the command:

```
# imta dirsync [ other options ... ]
```

Finally, check that the ownership of all files in `/var/opt/SUNWmail/imta/db` is set to inetmail. Verify that all the files are writable by the owner.

Multiple Reprocess Jobs Generated

If you are having severe performance problems, check if multiple process jobs are being generated. The `imta process<ret>` command should show only a single process running. If more are showing, look in `/etc/opt/SUNWmail/imta/aliases`, and verify that it contains the following line:

```
postmaster: <user-name>@FQDN
```

Make sure the postmaster address is valid and is receiving mail. If it doesn't, add this line and do a fresh restart of the IMTA.

```
# imta restart
```

Addresses Not Reversed

The IMTA has the ability to reverse envelope `from:` and `header` addresses. Generally, this is used to turn the address form `username@host.domain` to the more public form `first_name.last_name@domain` so that recipients outside of the domain only see the latter form.

This functionality is not always activated. For instance, it is not active if the routability scope is set to Local System Users Only. To enable, set the option `USE REVERSE DATABASE` to `5` in `/etc/opt/SUNWmail/imta/option.dat`, and make sure the list of channel keywords for the delivery channel does not contain `noreverse`.

Another cause of reverse address failure is the absence or incorrect configuration of the `mail` LDAP attribute.

To further diagnose the problem, set `MM_DEBUG` to `5` in `option.dat` and activate the slave diagnostic output for the queuing channel. Restart the IMTA and reproduce the problem. Examine the debug output file created in `/var/opt/SUNWmail/imta/log`. For information on how to use diagnostic output, see "To Configure Diagnostics Output" on page 105.

SMTP Access Restrictions Not Working As Expected

Common reasons for such problems include:

1. Interference between access control rules and rewrite rules. The address is rewritten before it is processed by the access rules, and the access rules handle the original and rewritten addresses differently.

2. Interference between access rules. A typical case arises when a message is blocked using IP addresses only. Other rules involving addresses are never applied since IP level envelope information is sufficient to make an access decision.

The problem can best be diagnosed using the debugging functionality. See "To Configure Diagnostics Output" on page 105. For further details on access restriction, refer to the *SIMS Reference Manual*.

Troubleshooting the Directory Service

Diagnosing SIMS Problems Caused by Improper Directory Entries

Because SIMS relies completely on the presence and values of certain attributes in the directory, the single most common set of problems installing and maintaining SIMS is with LDIF generated by sources other than `imldifsync`, or by `ldapmodify` if accurate information is not entered into the SIMS install HTTP forms. This section discusses some common problems caused by incorrectly configuring attributes, and provides hints in diagnosing them.

General Hints

LDIF-generating scripts should be careful not to accidentally include nonprinting characters or white-space characters in attribute values. This is most commonly seen when a space (‘ ‘) is added at the end of an attribute value when not appropriate. For example, you should enter the value for `mailFolderMap` as:

```
“mailFolderMap: SUN-MS”
```

and not as:.

```
“mailFolderMap: SUN-MS ”
```

where the quotes show the inappropriate spaces.

It is always best to try and scope a particular problem before trying to diagnose it. This may sound obvious, but within the context of SIMS this means:

- If some users are having problems, dump the LDIF for users that are known to work (using `ldapsearch(1)` or the Admin Console) and compare this with the entries of users that do work.

- If data was added with an LDIF generating script, or even with `imldifsync`, for users that don't work, try adding the same information via the Admin Console. If this works then look for white space or unprintable characters and determine if they are being added by the LDIF-generating scripts.

Users Can't Log In to Their IMAP Mail Server

Check the following attributes:

- `userPassword` - Should match the encrypted password entry in `/etc/passwd` or the equivalent. Note that this will not be true if the attribute is changed directly some time after the directory has been in use for a while.
- `uid` - Should match the `uid` in `/etc/passwd` or the equivalent.
- `mailFolderMap` - This currently has only one of two valid values: "Sun-MS" for users receiving mail via the SIMS messages store, and "UNIX V7" for users who use the `/var/mail` inbox format.

Mail Inbound to the SIMS MTA Bounces

Check the following attributes:

- `rfc822Mailbox` - Should have valid `user@FQDN` (fully qualified DNS domain name) value.
- `mailDeliveryOption` - Mailbox, native, program, forward, and file for users; shared, program, and file for groups.
- `mailFolderMap` - Must be set to UNIX V7 (`/var/mail`) or Sun-MS as appropriate.

Mail Delivered Does Not Arrive

- `mailQuota` - Set incorrectly.
- `mailFolderMap` - Must be set to UNIX V7 (`/var/mail`) or Sun-MS as appropriate.

Mail Forwarded between SIMS and Other Servers Isn't Received

- `mailForwardingAddr` - Not set or set incorrectly.

Re-generating the Sun Directory Service Directory Index

Index re-generation is done by running the dsidxgen tool. The command takes the following arguments:

```
# dsidxgen [backend_directory] [-a attribute_name
[attribute_name...]]
```

If backend_directory is not specified then dsidxgen regenerates index for all data stores defined in the SunDS 3.1 configuration files. The list of attributes for which to regenerate indexes are specified by -a attribute_nam'. If not supplied then all indexes are generated apart from id2children.dbb, dn2id.dbb, id2entry.dbb, dn.dbb and objectclass.dbb.

Crash Recovery

▼ SIMS Crash Recovery

If your mail server becomes nonfunctional, you must perform the following procedure:

1. **Enter the following command as root:**

```
# imta queue-recover_crash
```

This command invokes a utility that rebuilds the queue caches for the Sun Message Store and /var/mail. These caches may become corrupted during the time that the mail server becomes nonfunctional. For example, a message may be partially written to the Sun Message Store cache during the time that the mail server becomes nonfunctional. Running the utility will enable the mail server to clean up these types of corruption.

2. **Stop any components that might still be running by entering the following:**

```
# /etc/init.d/im.server stop
```

3. **Start all components by entering the following:**

```
# /etc/init.d/im.server start
```

Message Store Crash Recovery

In the event of a catastrophic system failure, the message store may be left in an inconsistent state and in some instances require data recovery from backup media. If you see the following message, it means that SIMS did not start and the store was shut down abnormally:

```
/var/log/syslog.1:Oct 2 16:40:24 mcm-nitro
SUNWmail.ims.imaccessd[1373]:Message store may be inconsistent.
Please run imcheck -c
```

Follow the procedure below to recover the message store.

1. **Change to the proper directory:**

```
% cd /opt/SUNWmail/sbin/imta
```

2. **Make sure IMTA is not running. To stop the IMTA, run:**

```
% imta stop
```

3. **Make sure `imaccessd` is not running. To stop the `imaccessd`, run:**

```
% mt.scheduler stop
```

Note – The `imaccessd` process should never be killed using the `kill -9` command. If this should accidently occur, run `imcheck -c` before restarting `imaccessd`.

---

4. **Run the following as `root`:**

```
% imcheck -c -f <filename>
```

   a. **If `imcheck` completes successfully, check the `/var/opt/SUNWmail/ims/adm/restore_log` file. If this file is present, restore the users whose names are in this file, and then remove the file. For example:**

```
% imrestore -i
% rm /var/opt/SUNWmail/ims/adm/restore_log
```

   b. **If `imcheck` fails, save the syslog file and the store report, then contact your Sun Service Provider. The store report is at `/var/opt/SUNWmail/ims/adm/<filename>`. Do not restart the MTA and `imaccessd`.**

Admin Console Crash Recovery

If the Admin Console hangs, kill the browser process, restart the browser, and reconnect to the Admin server. If the Admin Console crashes or vanishes, restart the browser and reconnect to the Admin Server. Note that switching back and forth between pages may cause Admin Console to hang or crash while communicating with the Admin server. To kill a browser process on Solaris, perform the following steps:

1. **Find the process id.**
2. **Bring up a UNIX shell window and type the following command as root:**

```
# ps -ef | grep netscape <cr>
```

You will see something like this:

```
myuid 350 10767  0 hh:mm:ss pts/x    0:00 grep netscape
root 26145     1  0 hh:mm:ss pts/x    0:46 /usr/netscape,v4.51/bin/netscape
                       -Dlegacy.host= -Ddirectoryhost=motmot
                       -Dconsole.domain=eng.bridge
myuid 336 10767 24 hh:mm:ss pts/x    0:15 /usr/dt/appconfinetscape/
                       runtime/bin/sparc/green_threads/jre -classpath ..
```

3. Kill the browser process using the following command:

```
# kill <browser process number (in this case 336)> <cr>
```

4. On rare occasions the Admin Server will crash and you may need to restart the administration server using the following command:

```
# /opt/SUNWmail/sbin/adm.server stop
# /opt/SUNWmail/sbin/adm.server start
```

Note – For Win 95 and NT environments, please refer to the corresponding administrator’s guides for instructions on killing a browser process.

APPENDIX **A**

Configuring SIMS as a Proxy Message Access Server

Proxy Message Access Servers Overview

A *proxy message access* server differs from a regular SIMS server in that instead of serving the POP/IMAP requests itself, it forwards the request to the message access server with the requested mail folders (FIGURE A-1). The proxy may or may not have a local message store, but it acts as a virtual message access server by forwarding POP/IMAP requests to the appropriate message store. Message access proxies are useful for a number of reasons such as horizontal scalability and internet access to private intranet mail systems. These are discussed in “Proxy Server Models” on page 303.

Proxies accept client POP/IMAP requests for mailbox access and authenticate requestor’s passwords. The proxy’s mail access daemon (`imaccessd`) forwards the request to the appropriate mail access server (i.e., the server containing the desired mailbox). The requestor is again authenticated by the mail access server where the mailbox resides. At this point, the proxy acts as a simple pipe between the client and the mail server, forwarding whatever one sends to the other, until either the client or the server closes the connection.

Although a proxy server may not have the requested message store, from the client’s point of view, the proxy acts like the real mail access server. Because the proxy communicates with the requested mail server using POP/IMAP, from the requested mail access server’s point of view the proxy appears as another mail client.

SIMS message access proxies have two configurations, a *pure proxy*, which acts only as a proxy for SIMS mail servers, and a *message access proxy/message access server* which can act as a proxy for some mail addresses and as a full mail server for local addresses. An example of these is shown in FIGURE A-1.

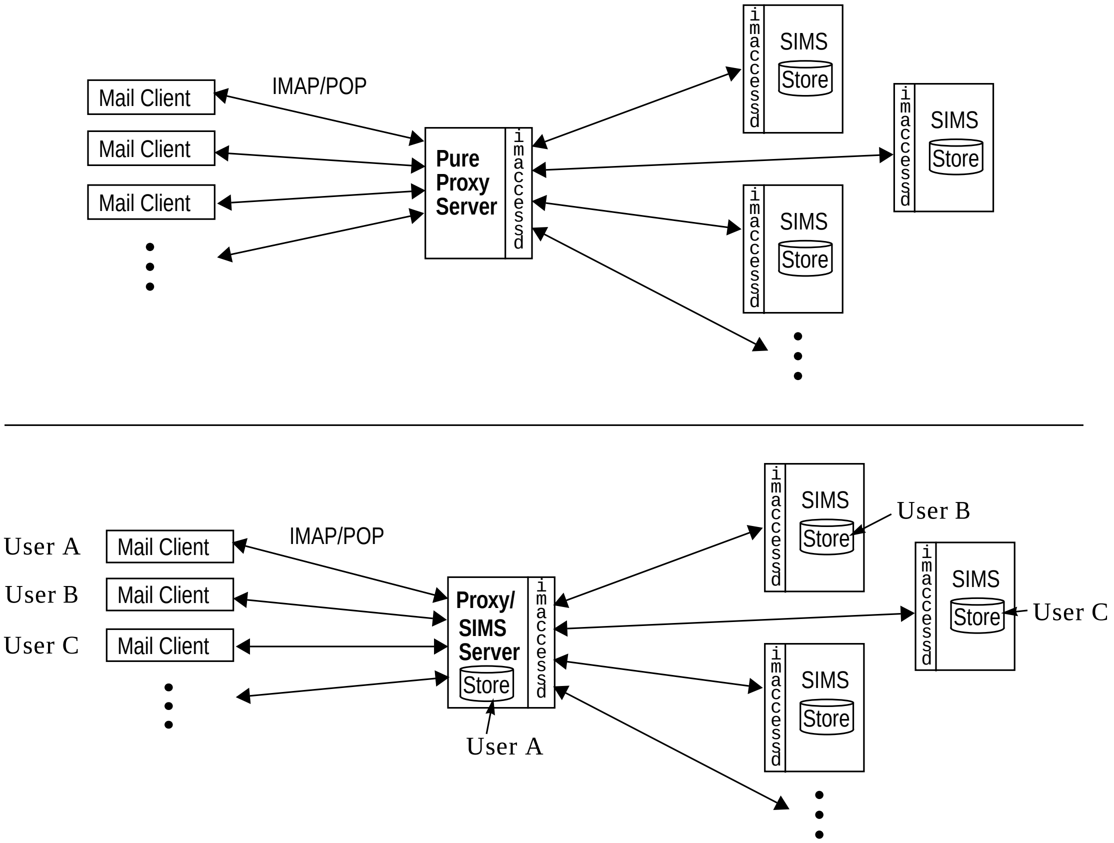


FIGURE A-1 Pure Proxy Server and Mail Access Proxy+Mail Access Server

Proxy Server Models

Proxy servers are useful for a number of applications. How you deploy proxy servers depends on the configuration of your email system and what your goals are. This section describes three possible scenarios and models where proxy servers could be used.

Proxy Servers for Horizontal Scalability

Horizontal scalability is the ability to expand the capacity of a SIMS environment by adding more servers. Proxy servers make horizontal scalability possible by having clients point to a single host name which provides access to their mail. Proxies do the work of routing the protocol traffic to and from the appropriate Message Store server. Since proxies allow clients to access their mail folders through a host name which is independent of the actual message store host name, capacity can be added without any burden or reconfiguration on the clients. (For example, having to reconfigure the message access server on each client.)

You may not want to have a single SIMS server supporting the hundreds of thousands of users that Internet Service Providers (ISPs) need to support. Without proxy servers, each user would have to specify their server host name to retrieve mail. By using proxy servers, messages can be accessed through one virtual mail server, while any number of actual mail servers perform actual message storage and retrieval.

By offering only one single virtual mail server, ISPs can add additional mailbox capacity by simply adding more servers behind the proxies.

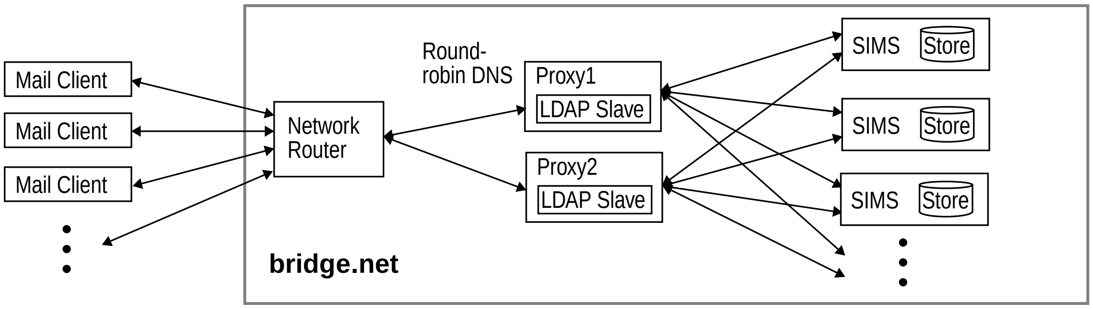


FIGURE A-2 Proxy Server in an ISP Environment

In the figure above, users log in to the system using the domain name, `bridge.net`. Mail requests are routed through the system and sent to a proxy via round-robin DNS (DNS that can return more than one IP address in round-robin fashion to distribute load among multiple proxy servers). The proxy authenticates the user through a replicated LDAP directory, then sends the request to the appropriate message access server. Additional capacity is achieved by adding more message access servers behind the proxies.

This deployment allows for easy expansion of capacity and, by virtue of round-robin DNS, allows proxies to be treated as field replaceable units. If `bridge.net` needs to expand message store capacity to accommodate new customers, they can do so either by expanding the capacity of an existing Message Store server by adding system resources, or they can add a new Message Store server. In either case, clients will not be required to change their mail server hostname setting.

Proxy Servers for the Internet Mail Access

A company that protects its network behind a firewall could, by using a proxy server, allow employees to access their e-mail outside the firewall through the global internet instead of having to maintain a private modem-pool to connect to the private intranet directly.

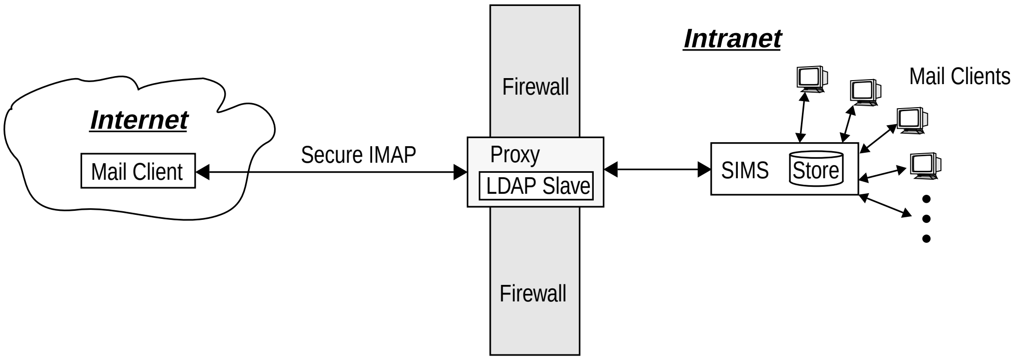


FIGURE A-3 Proxy Server for Internet Access

In the figure above, an internet mail client accesses his mail through a proxy server on the firewall via a secure IMAP connection. The proxy authenticates the user, then forwards mail store requests to the SIMS message store server. The SIMS then sends message data to the proxy which forwards it to the mail client.

Proxy Servers for Migrating Users

As an organization grows, additional SIMS servers may be added, and users may be migrated from an old server to a new server. As users are migrated, it would be nice if they could maintain the same server domain address rather than have to adopt a new domain address.

This can be done by activating the message access proxy feature on the SIMS Server. When migrated users make mail access requests, the proxy will forward their requests to the new server. Local users will continue to have their requests serviced at the local host.

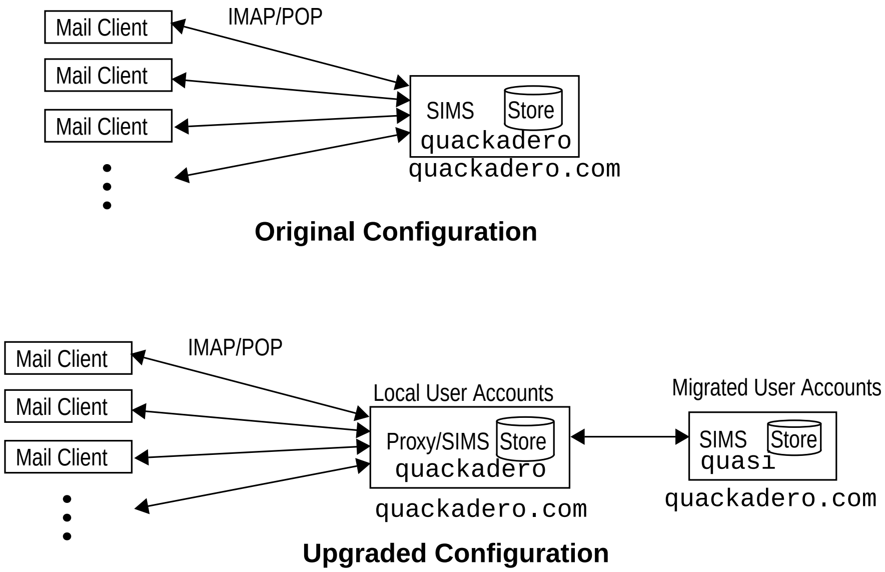


FIGURE A-4 Proxy+Mail Server for Migrating Users

In FIGURE A-4 the top drawing shows the company's original email configuration. Users connect to a server called *quackadero* and access mail using the server name `quackadero.com`. In the bottom drawing, quackadero has been converted from a regular mail server to a message access proxy / message access server, and a new server called *quasi* has been added with a number users having been migrated to quasi. However, even though these users are now on quasi, they can still access their mail using the same `quackadero.com` domain name. quackadero provides service for users whose account it supports and forwards mail store requests for users supported by quasi.

How to Deploy a SIMS Message Access Proxy

The first step in deploying a SIMS proxy model at your site is to choose a model which will address the issues and problems you face. In this section we will describe how to deploy a pure proxy and a proxy+mail server within an organization. We will not specifically describe proxy deployment for horizontal scalability since how this is done will depend upon the platform used for the round-robin DNS which will differ from site to site.

Setting Up a Pure Proxy

In this section we will describe a generic configuration of a pure message access proxy. Details, such as where in relation to the firewall your proxy is placed or the configuration of a round-robin DNS server for a multiple proxy setup, will not be described.

Proxies need to be configured with the SIMS directory service before they can be operational. The proxy uses the directory to authenticate users and forward requests to the appropriate message store server. The proxy directory must be designated as a replicated slave to the master SIMS directory located on one of the mail servers. This is depicted in FIGURE A-5. It is possible to configure the proxy to use an LDAP server on a different machine (refer to the `ims-ldap-server` parameter in the `sims.cnf` man page), but for performance reasons, it is preferable to have a local LDAP replica on the proxy.

Note – Caution! The master and slave server must have the same replication configuration for the updates to work properly. The master and slave must also have the same schema since replication between servers with dissimilar schemas may lead to unpredictable results. Also, `dsprepush` must be run on the system with the master server if it is to be replicated. See the *Sun Directory Services 3.1 Administration Guide*.

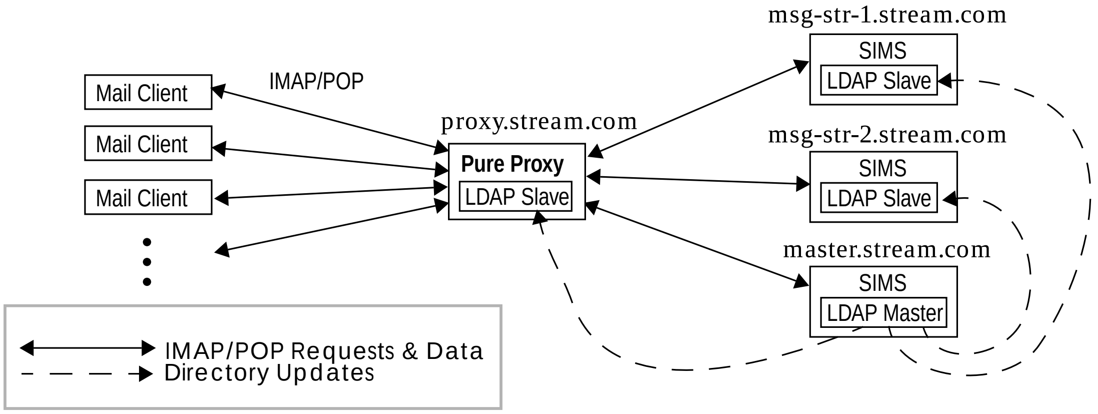


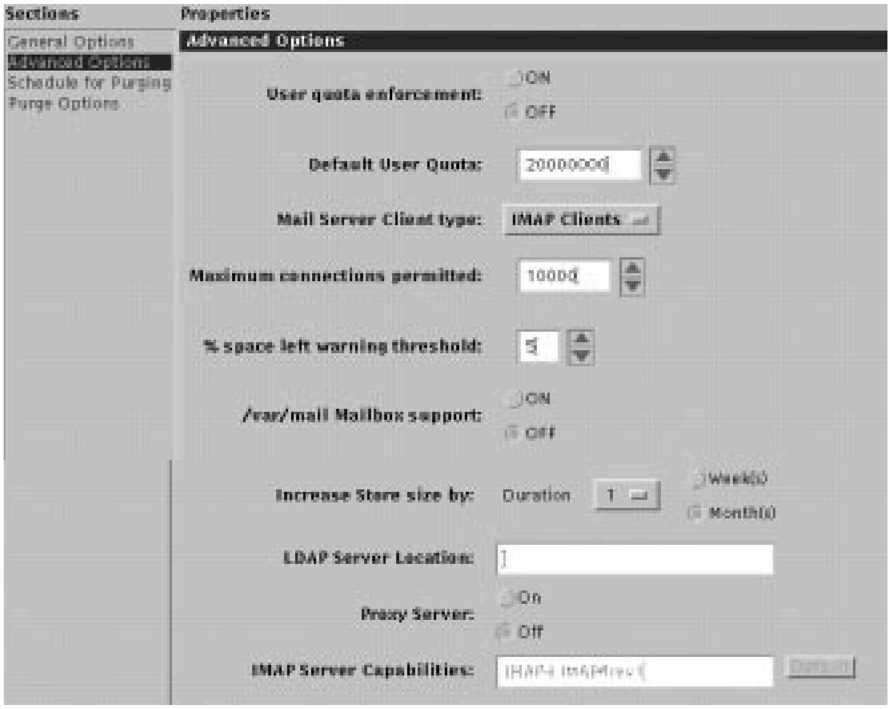
FIGURE A-5 Pure Proxy Mail System Showing Master to Slave Directory Updates

▼ To Configure a Pure Proxy

This section describes how to configure a pure proxy server as a replicated LDAP directory slave server. In this example the fully qualified proxy hostname is called `proxy.stream.com`. The master LDAP directory server is called `master.stream.com`.

1. **Install SIMS on the proxy machine**
2. **Configure this system to be a proxy server.**

   In our example you would bring up the Advanced Options of the Sun Message Store property book on `proxy.stream.com` and press the Proxy Server Button to On.



User quota enforcement: ○ ON ● OFF

Default User Quota: 20000000

Mail Server Client type: IMAP Clients

Maximum connections permitted: 10000

% space left warning threshold: 5

/var/mail Mailbox support: ○ ON ● OFF

Increase Store size by: Duration 1 ○ Week(s) ● Month(s)

LDAP Server Location:

Proxy Server: ○ On ● Off

IMAP Server Capabilities: IMAP4 IMAP4rev1 Default

FIGURE A-6 Message Advanced Options Section (Extended View)

3. **Configure the proxy to replicate a local directory from a master LDAP server (**FIGURE A-5**), or specify another LDAP server to serve as the directory server for the proxy.**

Note – The Sun Directory Services documentation can be found at http://docs.sun.com:80/ab2/coll.297.1/@Ab2CollToc?subject=sysadmin. The Netscape Directory Services documentation can be found at (http://home.netscape.com/eng/server/directory/

---

a. **To configure thenew proxy to replicate a local directory from a master LDAP server:**

The process will differ depending whether you use the Netscape or Sun Directory Server, however, the basic steps are the same.

i. **Create naming contexts (subtrees) to be replicated.**

If you require OSI and DC naming contexts, create them both. OSI trees must be mapped to a DC tree refer to the schema section in the *SIMS Reference Manual*.

ii. **Specify the naming contexts to be replicated slaves and designate a master LDAP host server for the slaves.**

In our example, `master.stream.com` is designated as the LDAP master server to the LDAP slave `proxy.stream.com`. We'll assume we only have a DC tree and that the naming context to be replicated is `dc=stream,dc=com,o=internet`.

Refer to the directory service documentation for replication details.

b. **To specify another LDAP server to serve as the directory server for the proxy:**

If you choose this configuration, the proxy will not use a local directory server, but use a directory server on another machine. See the `imadmin-modify-currentldap` man page.

4. **Create a new replica from the master LDAP server.**

Go to the master LDAP server and create a new replica of the naming context to be replicated. Specify the naming context to be replicated and the host that will act as a replicated slave. In our example, the replicated naming context is `dc=stream,dc=com,o=internet` and the replicated slave is `proxy.stream.com`. Again, if there are mirrored OSI and DC naming contexts, you'll need to create replicas for both.

5. **Initialize the replica.**

How this process is done will differ depending whether you are using the Netscape or Sun Directory Services.

6. **Synchronize the replica and set synchronization schedule.**

At this point you have set up a LDAP slave and configured its LDAP master to create a replica for the slave. You now need to synchronize the slave directory with the master directory and set up a synchronization schedule for the updates. (Refer to directory service documentation.

7. **When synchronization occurs, the proxy is operational.**

▼ To Configure IMAP Capabilities in the Proxy

Note – Read this section if you are configuring a SIMS proxy with a non-SIMS back end mail server.

CAPABILITY is an IMAP command that lists commands in addition to the standard (RFC2060) commands that a given server will support. Since CAPABILITY is valid even before the client has been authenticated (capabilities can include authentication mechanisms), the proxy has no way of knowing in advance to which server the user will be connected to, and therefore can't list the capabilities supported by this server.

So, when the proxy is enabled in imaccessd, the only capabilities that will be returned to the client when capability is executed are:

```
* CAPABILITY IMAP4 IMAP4rev1
```

plus the authentication mechanisms supported by the proxy.

This means that all the remote server(s) MUST support IMAP4 and IMAP4rev1. If you have servers connected to the proxy that do not support both protocols, or, if you need to have the proxy advertise capabilities supported by the real servers, then you need to define the parameter ims-caps-proxy in /etc/opt/SUNWmail/ims/ims.cnf that will contain these capabilities. This can also be done in the Admin Console (see "To Configure IMAP Capabilities in the Proxy" on page 310).

This parameter, if absent, is equivalent to IMAP4 IMAP4rev1. You can disable either IMAP4 or IMAP4rev1 if the back end server doesn't support both, or you can add new capabilities to the list.

One caveat: some additional capabilities include commands that are supported once the client is authenticated (example: the SCAN command in SIMS). There is no harm in advertising these in the proxy since the client can only issue them at a time the real server will receive and process them. However, for some extensions that enable a behavior of the server (such as IMAP4SUNVERSION in SIMS), it is not recommended that you add these to the list because the client could send the command before authentication is completed, and the proxy server would not forward the command to the real server.

Setting Up a Proxy+Mail Server

This section describes how to convert a SIMS mail server to a message access proxy/ message access server. We will use the hypothetical example of an administrator migrating a number of users on the original SIMS mail server to a new SIMS server, and converting the original SIMS mail server to a proxy/message access server (FIGURE A-4 on page 306). The basic steps for completing these steps are as follows:

1. Install new SIMS machine.
2. Convert the old SIMS machine to a proxy+mail server.
3. Confiure the new machine as a slave LDAP server, and configure the old machine to be a master server.

4. Temporarily disable mailbox accounts of users who are to be migrated and send incoming mail to the Hold Channel for temporary storage.

5. Using the command `imbackup` and `imrestore`, migrate the users from the old machine to the new machine.

6. Change the `Mailhost` attribute in the entries of the migrated users

7. Enable the disabled mailbox accounts so that they can receive mail.

8. Delete all the migrated accounts from the old machine.

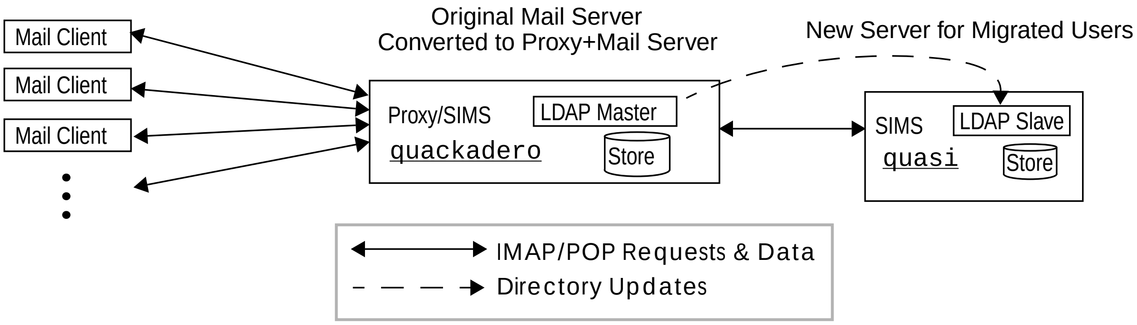


FIGURE A-7 Converting Mail Server to Proxy+Mail Server.

▼ To Migrate Users by Converting a Mail Server to a Proxy+Mail Server

1. **Install new SIMS host.**

2. **Convert the old SIMS host to a SIMS proxy+mail host.**

   Bring up the Admin Console on the old SIMS host. Go to the Advanced Options section in the Message Store property book (FIGURE A-7). Press Proxy Server On button. Also, set the IMAP Server Capabilities. This is typically `IMAP4 IMAP4rev1`, which you can enter by pressing the Default button (see “To Configure IMAP Capabilities in the Proxy” on page 310 for additional information). You must stop then start the message access protocols (see “Message Access Protocol Connections” on page 176).

3. **Populate the new machine with the directory information.**

   For example, configure the new machine as an LDAP slave server and the old machine (now a proxy+mail server) as an LDAP master server. Follow the instructions described in “To Configure a Pure Proxy” on page 308.

4. **Temporarily disable mailbox accounts of users who are to be migrated so that mail sent to these users will be put on hold until the accounts are restarted.**

   For each user and group LDAP entry to be migrated, add the value `mailDeliveryOption`: `hold` (you do not have to remove the other `mailDeliveryOption` values like `mailbox`). Run an `imta dirsync` to synchronize the alias table. Execute the command `hold_slave` to send incoming mail to the Hold Channel. (See the section on the Hold Channel in the *SIMS Reference Manual* and the `hold_slave` man page).

5. **Migrate mailboxes from one machine to another.**

   a. **Identify users to be moved to the new machine and have these users log out of their mail clients.**

      They must not use their mail client until after migration is complete.

   b. **Use** `imbackup -f bak -u username_file` **to backup the mailboxes to be migrated.**

      `bak` is the name of the file in which to back up the mailboxes. `username_file` is a file containing a list of user names to be migrated. Each name must be separated by spaces, tabs, or carriage returns. See the `imbackup` man page for details.

   c. **Use** `imrestore -t3 -f bak -u username_file` **to restore the backed up mailboxes to the new SIMS machine.**

6. **Change the** `Mailhost` **attribute in the entries of the migrated users and groups.**

   You can do this from the Admin Console (see "To Modify a User Entry" on page 41 and "To Modify a Group Entry" on page 49). You can also use the `ldapmodify` command if you prefer to do this in a UNIX script. See `ldapmodify` man page for details.

7. **Enable the disabled mailbox accounts so that they can receive mail.**

   For each user and group LDAP entry migrated, remove the `mailDeliveryOption`: `hold` value and run `imta dirsync`. Execute the command `hold_master` to deliver message in the Hold Channel to the migrated mailboxes. (See the section on the Hold Channel in the *SIMS Reference Manual* and the `hold_master` man page).

   Proxy+mail server should be running as planned.

8. **If the system is working, delete the migrated accounts from the old machine.**

   Use `imdeluser.`

APPENDIX **B**

Migrating Mailboxes from /var/mail to SIMS

This section discusses various techniques and strategies for migrating user mailboxes from `/var/mail` to SIMS. While there are many methods for migrating users from `/var/mail` to SIMS. The basic migration process is as follows:

1. Install SIMS on a new server
2. Populate the SIMS directory with the migrated users.
3. Kill the sendmail daemon.
4. Migrate the user mailboxes using `imimportmbox.`
5. Start the new SIMS server.

However, between the time of killing the sendmail daemon, and starting the SIMS server, the user's account is down. Mail sent to the user will be bounced back to the recipient, and the user will not be able to send mail. The challenge arises in trying to minimize downtime.

The mailbox migration methods you choose will depend on the following:

- How many users in your system?
- How important is minimizing down time? That is, how significant is it if the mail system is temporarily unavailable to the user and bounces incoming mail to back to the recipient?
- Are you willing to go through the extra complexity of installing SMTP Choke Routers in order to minimize the down time?

There are a number of ways to temporarily intercept and save mail sent to `/var/mail` and then send it to the new SIMS server. The remainder of this appendix describes three examples of migrating users with various levels of user transparency. These examples are meant to give guidelines for migrating mailboxes, and may or may not provide the best solution for your needs. Use these examples to learn and select the methods, techniques, and strategies that work best for your situation

▼ Example 1: Converting`/var/mail` to the Sun Message Store—Simplest

The example replaces an old sendmail server with a new SIMS server.

User transparency issues:

- When the system is brought down, users can neither send nor retrieve messages.
- Messages sent to the user are bounced back to the sender while the system is down.
- User clients must change the name of the new server toward which they point.

1. **Install and configure the new SIMS server.**

   Configure the Directory Server, IMTA, and Message Store as needed.

2. **Populate the Directory on the new SIMS server with the appropriate entries.**

   See Chapter 9, Populating SIMS with Users and Groups and the *SIMS Provisioning Guide* for more information.

   a. **Change the user's LDAP entry to include the new mailhost attribute.**

      For each entry set the `mailhost` attribute to fully-qualified name of the new SIMS server.

3. **Run a full `dirsync`.**

   See the `imta-dirsync` man page for details.

4. **Bring down the old sendmail server.**

   Kill the sendmail server daemon (or whatever server daemon you are using).

5. **Migrate `/var/mail` mailboxes from old server to new server.**

   Run `imimportmbox` to migrate mailboxes to the new server in the Sun Message Store format.

6. **Make sure the user's mail clients now point to the new server.**

7. **Start up the new SIMS server.**

   ```
   im.server start
   ```

▼ Example 2: Converting `/var/mail` to the SIMS Message Store Using an SMTP Choke Router or `.forward`

This example replaces a sendmail host with a new SIMS server. Mail arriving while the system is down is sent to either an SMTP choke router or a `.forward` file.

User transparency issues:

- Users being migrated will temporarily prevented from accessing their mailbox or sending mail.
- Messages sent to the user are saved in either a SMTP choke router or .forward file. No messages are bounced.
- User clients must change the name of the new server toward which they point.
- Mail sent before the `/var/mail` messages are migrated will be dated and queued in the mail store with a delivery date earlier than the messages to be migrated. That is, your message delivery queue will look out of order.

1. **Install and configure the new SIMS server.**

   Configure the Directory Server, IMTA, and Message Store as needed.

2. **Save incoming mail to an SMTP choke router or a .forward file.**

   The SMTP choke router intercepts and temporarily saves incoming mail. After the mailboxes are migrated and the new server is set up, you can send the saved messages to the new message store.

   A `.forward` file forwards mail addressed to a specific user to specified file. After the mailboxes are migrated and the new server is set up, you can run a `imimportmbox` to migrate the `.forward` mail to the new server in the SIMS message store format.

3. **Populate the Directory on the new SIMS server with the migrated entries.**

   See Chapter 9, Populating SIMS with Users and Groups and the *SIMS Provisioning Guide* for more information.

   a. **Change the user’s LDAP entry to include the new mailhost attribute.**

      For each entry set the `mailhost` attribute to the fully-qualified name of the new SIMS server.

4. **Start up the new SIMS server.**

   ```
   /etc/init.d/im.server start
   ```

   Users can now send and retrieve new mail, but these mailboxes will not contain the old mail that has yet to be migrated.

5. **Temporarily disable a batch of user to migrate.**

   We recommend ~1,000. Set the `emailPersonStatus` attribute to `inactive` for each user entry. These users will not be able to access their mailboxes, or send mail. Incoming mail will be temporarily stored in the SMTP choke router of the `.forward` file.

6. **Migrate disabled `/var/mail` mailboxes from the old server to new server.**

   Run `imimportmbox` to migrate mailboxes to the new server in the Sun Message Store format.

7. **Make sure the user's mail clients now point to the new server.**

8. **Enable the migrated inactive users.**

   Set the `emailPersonStatus` attribute to `active` for each user entry.

9. **Send messages temporarily stored in SMTP choke router or to the `.forward` file to the new mailboxes.**

Note – New mail delivered either before or while `imimportmbox` is being run will appear in the mail store as having been delivered before migrated mail.

▼ Example 3: Converting `/var/mail` to SIMS Using a Proxy

This example installs SIMS on the current sendmail host and configures it to be a proxy. Another SIMS host is installed on the backend and configured as a message store host.

User transparency issues:

- Users being migrated will temporarily prevented from accessing their mailbox, however, they can still send mail.
- Messages sent to the user are saved in a temporary hold channel. No messages are bounced.
- User clients do not have to change the name of the server toward which they point, since they will still be accessing mail from the same machine, which is not a proxy.

1. **Install the new SIMS server.**

   Configure the Directory Server, IMTA, and Message Store as needed.

2. **Install SIMS on the current sendmail server and convert it to a SIMS pure proxy.**

   See "To Configure a Pure Proxy" on page 308.

3. **Populate the directories on the new SIMS servers with the new entries.**

   See Chapter 9, Populating SIMS with Users and Groups and the *SIMS Provisioning Guide* for more information. Note that the new servers will need to get updated directory information either as directory masters or slaves. (You can also specify another machine to serve as the directory server for either of the proxy or non-proxy machine. See the `imadmin-modify-currentldap` man page.)

4. **Change the `Mailhost` attribute in the entries of the migrated users and groups to the name of the new server.**

   You can do this from the Admin Console (see "To Modify a User Entry" on page 41 and "To Modify a Group Entry" on page 49). You can also use the `ldapmodify` command if you prefer to do this in a UNIX script. See `ldapmodify` man page for details.

5. **Temporarily disable mailbox accounts of users who are to be migrated so that mail sent to these users will be put on hold until the accounts are restarted.**

   For each user and group LDAP entry to be migrated, set the `mailDeliveryOption` to `hold`. Execute the command `hold_slave` to send incoming mail to the hold channel. (See the section on the hold channel in the *SIMS Reference Manual* and the `hold_slave` man page). During this time, users will not be able to access their mailboxes.

6. **Start up the new SIMS server and SIMS proxy, and kill the sendmail daemon.**

   Start up command: `im.server start`.

   Incoming and outgoing mail will now be handled by the new SIMS machines. However, incoming mail will go to the Hold channel instead of to the message store.

7. **Migrate `/var/mail` Mailboxes from old server to new SIMS server.**

   Use `imimportmbox` to migrate mailboxes to the new server in the Sun Message Store format. See the man page.

8. **Enable the disabled mailbox accounts so that they can receive mail.**

   For each user and group LDAP entry migrated, change the `mailDeliveryOption` setting from `hold` to `mailbox`. Execute the command `hold_master` to deliver message in the Hold Channel to the migrated mailboxes. (See the section on the Hold Channel in the *SIMS Reference Manual* and the `hold_master` man page).

   Proxy / mail server should be running as planned.

9. **If the system is working, delete all the migrated accounts from the old machine.**

   Use `imdeluser`.

APPENDIX **C**

Populating the Directory Examples

Populating the Directory with User Data—Sample Session

Alpha Corporation is setting up a pilot test of the directory with two users on a lab machine called `testserver`. The test machine uses NIS+, and has the following users defined:

```
jdoe:fWFuXyZ1S..Vk:1001:10:John Doe:/export/home/jdoe:/bin/sh
gevert:fWFuXyZ1S..Vk:1002:10:Gail Evert:/export/home/gevert:/bin/sh
```

To create directory entries for these users, complete the following steps:

1. **Log in as root.**

```
$ su
Password: <Enter your root password>
#
```

2. **Use the `getent` command to save the user entries in a file:**

```
# getent passwd > /tmp/passwd
```

3. **Use the `niscat` command to extract user information from the mail aliases file, and use the `sed` command to format the data:**

```
# niscat mail.aliases > /tmp/aliases.tmp
# sed 's/ /: /' /tmp/aliases.tmp > /tmp/aliases
```

4. **Change directories to the location shown and edit the `imldifsync.conf` file.**

```
# cd /etc/opt/SUNWmail/dir_svc
# vi imldifsync.conf
```

5. **Change the `mail-server`, `passwd-file` and `aliases-file` values, and uncomment the `mode = users` line as shown:**

```
mail-server = "<mailserverhostname>.<fully qualified domain name>"
passwd-file = "/tmp/passwd"
aliases-file = "/tmp/aliases"
mode = users
```

In the above example, your `mail-server` can be `testserver.eng.alpha.com`., where `testserver` is the host name of the SIMS mail server. In `/etc/opt/SUNWmail/dir_svc` there will be two files:

`imldifsync.users.conf`
`imldifsync.groups.conf`

6. **Change directories to the location shown and convert the user data to LDIF format.**

   Use the `imldifsync` command to generate formatted user data files (`LDIF` files).

```
# /opt/SUNWmail/sbin/imldifsync -c imldifsync.users.conf > /tmp/
users.ldif
```

   You will see the following results on the screen:

```
==================Statistics========================

Added DNs: 2
Modified DNs: 0
Delete DNs:   0

====================================================
```

Note – By default, the mail folder will be set to the Sun Message Store.

The file `users.ldif` contains the following

CODE EXAMPLE C-1 Contents of the `users.ldif` File *(1 of 2)*

```
dn: cn="John Doe (jdoe)",ou=People,o=Alpha,c=US
changetype: add
cn: John Doe (jdoe)
cn: John Doe
sn: Doe
initials: JD
givenName: John
rfc822MailAlias: john.doe@testserver.Alpha.COM
rfc822MailAlias: jdoe@testserver.Alpha.com
mail: jdoe@testserver.Alpha.COM
mailDeliveryOption: mailbox
mailHost: testserver.Alpha.com
userPassword: {crypt}fWFuXyZ1S..Vk
uid: jdoe
dataSource: imldifsync 1.0
objectClass: top
objectClass: inetOrgPerson
objectClass: organizationalPerson
```

CODE EXAMPLE C-1 Contents of the `users.ldif` File *(2 of 2)*

```
objectClass: person
mailQuota: -1
mailFolderMap: SUN-MS

dn: cn="Gail Evert (gevert)",ou=People,o=Alpha,c=US
changetype: add
cn: Gail Evert (gevert)
cn: Gail Evert
sn: Evert
initials: GE
givenName: Gail
Rfc822MailAlias: gail.evert@Engineering
Mail: gail.evert@testserver.Alpha.COM
mailDeliveryOption: mailbox
userPassword: {crypt}fWFuXyZ1S..Vk
uid: gevert
dataSource: imldifsync 1.0
objectClass: top
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
mailQuota: -1
mailFolderMap: SUN-MS
```

7. **Change directories to the location shown and populate the directory with the user LDIF formatted data.**

   Use the `ldapmodify` command to add the new entries to the directory:

```
# cd /opt/SUNWconn/bin
# ldapmodify -D "cn=admin,o=Alpha,c=us" -w secret -f /tmp/users.ldif
```

You will see the following output on the screen:

```
adding new entry cn="John Doe (jdoe)",ou=People,o=Alpha,c=US
adding new entry cn="Gail Evert (gevert)",ou=People,o=Alpha,c=US
```

8. **Verify that the entries are present in the directory, using the `ldapsearch` command.**

CODE EXAMPLE C-2 Results of the `ldapsearch` Command for User Data

```
# ldapsearch -L -b "o=Alpha,c=us" "cn=*" cn
dn: CN=John Doe (jdoe),OU=People,O=Alpha,C=US
cn: John Doe (jdoe)
cn: John Doe
dn: CN=Gail Evert (gevert),OU=People,O=Alpha,C=US
cn: Gail Evert (gevert)
cn: Gail Evert
```

Populating the Directory with User Aliases Data and Distribution Lists — Sample Session

The following example is a continuation from the user data population example shown in “Populating the Directory with User Data—Sample Session” on page 321. It also assumes that you have extracted the user mail-aliases information from NIS+ and are now attempting to populate the directory with user aliases data for Alpha Corporation, Inc. as shown below. The user mail-alias being created is called `testsubject` and it will have two people as its members, John Doe and Gail Evert. The owner of the alias is designated as `admin`. The distribution list mail-alias is called `testsubject-list`, and it has owner `owner-testsubject-list` and automated request alias `testsubject-list-request`. The owner is user `jdoe` and the distribution list has two members, `gevert` and `jdoe`.

```
testsubject: gevert,jdoe
owner-testsubject: admin

testsubject-list: jdoe,gevert
testsubject-list-request: jdoe
owner-testsubject-list: jdoe
```

To create directory entries for these user aliases, complete the following steps:

1. **Log in as root.**

```
$ su
Password: <Enter your root password>
#
```

Note – Since you have to populate the directory with user data before you populate it with user aliases data, and since the process of extracting user, user aliases, and distribution list data is the same, you have already completed Step 3 to Step 5 as part of Populating the Directory with User Data—Sample Session.” This section does not repeat these steps.

---

2. **Copy the `imldifsync.conf` file to `groups.conf` to keep the user population data distinct from the user aliases population data:**

```
# cp imldifsync.conf imldifsync.groups.conf
```

3. **Change directories to the location shown and convert the user aliases list data to LDIF format.**

   Use the `imldifsync` command to generate formatted user aliases data files (`LDIF` files).

```
# /opt/SUNWmail/sbin/imldifsync -c imldifsync.groups.conf > /tmp/
user_aliases.ldif
```

You will see the following results on the screen:

```
==================Statistics========================

Added DNs: 2
Modified DNs: 0
Delete DNs:   0

====================================================
```

Note – By default, the mail folder will be set to the Sun Message Store.

The file `user_aliases.ldif` contains the following:

CODE EXAMPLE C-3 Contents of the `user_aliases.ldif` File for User Aliases

```
dn: cn="testsubject",ou=Groups,o=Alpha,c=US
changetype: add
cn: testsubject
mail: testsubject@Alpha.com
rfc822MailMember: gevert@testserver.Alpha.COM
rfc822MailMember: jdoe@testserver.Alpha.COM
inetMailGroupVersion: 1.0
inetMailGroupStatus: active
mailDeliveryOption: mailbox
mailHost: mail.alpha.com
ownerDeliveryOption: mailbox
dataSource: imldifsync 1.0
objectClass: top
objectClass: inetMailGroup
objectClass: inetMailRouting
objectClass: groupOfUniqueNames

dn: cn="testsubject-list",ou=Groups,o=Alpha,c=US
changetype: add
cn: testsubject-list
mail: testsubject-list@Alpha.com
rfc822MailMember: gevert@testserver.Alpha.COM
rfc822MailMember: jdoe@testserver.Alpha.COM
inetMailGroupVersion: 1.0
inetMailGroupStatus: active
mailDeliveryOption: mailbox
mailHost: mail.alpha.com
ownerDeliveryOption: mailbox
dataSource: imldifsync 1.0
objectClass: top
objectClass: inetMailGroup
objectClass: inetMailRouting
objectClass: groupOfUniqueNames
```

4. **Change directories to the location shown and populate the directory with the user aliases LDIF formatted data.**

   Use the ldapmodify command to add the new entries to the directory:

```
# cd /opt/SUNWconn/bin
# ldapmodify -D "cn=admin,o=Alpha,c=us" -w secret -f /tmp/user_aliases.ldif
```

   You will see the following results on the screen:

```
adding new entry cn="testsubject",ou=Groups,o=Alpha,c=US
adding new entry cn="testsubject-list",ou=Groups,o=Alpha,c=US
```

5. **Verify that the entries are present in the directory, using the** ldapsearch **command.**

CODE EXAMPLE C-4 Results of the ldapsearch Command for User Aliases Data

```
# ldapsearch -L -b "o=Alpha,c=us" "cn=*" cn
dn: CN=testsubject,OU=Groups,O=Alpha,C=US
cn: testsubject
# ldapsearch -L -b "o=Alpha,c=us" "cn=*" cn
dn: CN=testsubject-list,OU=Groups,O=Alpha,C=US
cn: testsubject-list
```

Migrating /var/mail Mailboxes

The imimportmbox utility migrates /var/mail files into the message store. You need to determine which /var/mail files to transfer, since these files might be in a variety of places depending on the organization of the previous system. For a complete description on mailbox migration procedures, refer to Appendix B, “Migrating Mailboxes from /var/mail to SIMS.”

The imexportmbox utility can be used to copy email back out from the message store to disk in /var/mail format. But an export may not be the same byte for byte as an import, since imimportmbox parses /var/mail into the message store format and imexportmbox recreates a valid /var/mail file, which are not exactly the same.

For more information on imimportmbox or imexportmbox, see the man pages.

APPENDIX **D**

Error Messages

User Management Error Messages

`Fails to add/modify entry`

The connection to the directory server might be down. The Admin Server might need to be restarted.

`Cannot add the following entry ...`

The connection to the directory server might be down. The Admin Server might need to be restarted.

`Cannot access Content Manager`

Admin server might be down. Restart Admin Server.

`Failed to delete entry:`

The connection to the directory server might be down. The Admin Server might need to be restarted.

`... does not exists in the directory`

Directory structure might be inconsistent. Check the DN to make sure the node exists in the directory.

`Contains invalid input value.`

Check the indicated field to make sure it contains the valid information.

`Search failed`

The connection to the directory server might be down. The Admin Server might need to be restarted.

`Cannot find Administrative Server`

Admin server might be down. Restart Admin Server.

`Cannot find main Admin Console`

Admin Console is not connected. Try go back to the main login page and go through the login process.

`Create group failed`

The connection to the directory server might be down. The Admin Server might need to be restarted.

`Cannot find owner DN`

Inconsistent directory information. Manual inspection of the directory is required.

`Cannot access session`

Admin Console is not connected. Try go back to the main login page and go through the login process.

`Create group failed due to RMI error`

Transport error. Try restart the HotJava browser.

`Cannot find moderator DN`

Inconsistent directory information. Manual inspection of the directory is required.

`Parent node does not exist: ...`

Inconsistent directory information. Manual inspection of the directory is required.

`Cannot authenticate to LDAP server: ...`

The directory server might be down. Restart the directory server

`Failed to initialize LDAP library: ...`

The LDAP client library is not found in the library search path. Check installation components.

```
Cannot connect to LDAP server: ...
```

The directory server might be down. Restart the directory server

```
Cannot delete entry because SMCS is using this context
```

The delete operation is stopped because the entry is under SMCS control. Please verify the operation.

```
Cannot delete root dn
```

User tried to delete the root folder from the Admin Console. Attempt to do this will result in attempt to remove “all” of the entries in the directory.

Log Manager Error Messages

```
You need to search logs before saving them.
```

You are attempting to save the current display before completing the search of log entries. Perform a search of desired log entries by selecting the desired search criteria then click the Search button. Log entries that match your specified criteria will display. Click on the Log Manager menu and select Save the current display.

IMTA Error Messages

These messages may occur while using the IMTA and IMTA channel property books.

IMTA Channel Property Book Error Messages

`IMTA is already running.`

You are attempting to start the IMTA when it is already running. If desired, you can restart the IMTA from the IMTA property book by clicking on the IMTA menu and selecting Restart IMTA, or Stop IMTA then Start IMTA.

`[Add channel] Channel name already exists.`

You are attempting to create a channel with a name that already exists. Specify a unique name for the channel you are attempting to create.

`Please select a channel`

From the Selected menu in the IMTA property book, you chose an option other than Monitor Queue but did not select a channel from the Channels section. Select a channel from the Channels section by clicking on it. Click on the Selected menu and choose the desired option.

`This channel is not configurable.`

You are attempting to configure an internal channel (reprocessing, conversion, and defragmentation channels). Internal channels cannot be configured using the Admin Console.

```
Invalid entry in field: Pattern: <> Please change the value
before continuing.
```

In the Rewrite Rules section of the IMTA channels property book, you have entered an invalid entry for the pattern or a blank pattern and clicked the Add button. Refer to "To Add, Delete, or Modify a Rewrite Rule" on page 110 for more information on the correct syntax for entering a pattern. Try to add the rewrite rule again.

```
Invalid entry in field: Template: <ddsdsd hhh> Please change
the value before continuing.
```

In the Rewrite Rules section of the IMTA channels property book, you have entered an invalid entry for the template and clicked the Add button. Refer to "To Add, Delete, or Modify a Rewrite Rule" on page 110 for more information on the correct syntax for entering a template. Try to add the rewrite rule again.

IMTA Start-up Failure Error Messages

These messages appear at the command line when the IMTA fails to start up. There are a number of general sorts of issues that can interfere with the running of a variety of IMTA components; such issues include general syntax errors in an IMTA configuration, or license problems, or disk/quota problems leading to trouble writing files. The following are some of the more common general error messages.

Note that the `imta test -rewrite` utility will give warnings of many such common issues and with more detailed error messages than some other components of the IMTA may display. So `imta test -rewrite` can be a useful diagnostic tool to see the type of error generated.

Specific IMTA components may also issue other error messages, specific to that component. So when you an encounter an error not described below, see also the documentation on the IMTA component in question.

`Compiled configuration version mismatch`

One of the functions of the `imta cnbuild` utility is to compile IMTA configuration information into an image that can be loaded quickly. The compiled format is quite rigidly defined and often changes substantially between different versions of the IMTA. Minor changes may also occur as part of mid-version releases.

When such changes occur an internal version field is also changed so that incompatible formats can be detected. When an incompatible format is detected the IMTA components will halt with the above error. The solution to this problem is simply to generate a new compiled configuration with the UNIX command,

```
# imta cnbuild -option
```

It is also a good idea to use the `imta restart` command to restart any resident IMTA server processes so they can obtain updated configuration information.

`File open or create errors`

In order to send a message, the IMTA needs to read configuration files and create message files in the IMTA message queue directories. Configuration files must be readable to the user, which generally implies world read access on the files in the IMTA table directory. During installation, proper protections are assigned to these files. The IMTA utilities and procedures which create configuration files also assign proper protections. If the files are protected by the system manager or other privileged user or through some site-specific procedure, the IMTA may not be able to read configuration information. This will result in “File open” errors or unpredictable behavior. The `imta test -rewrite` utility will report additional information when it encounters problems reading configuration files. See the `imta-test-rewrite` man page for information on using this utility.

If the IMTA appears to function from privileged accounts but not from unprivileged accounts, then file protections in the IMTA table directory are likely to blame. Check the protections on configuration files and their directories. The only files that should be protected against world read access in the table directory are the queue cache database or other channel option files which may contain password information.

“File create” errors usually indicate a problem while creating a message file in an IMTA message queue directory. See “Check Message Queue Directories” on page 279 for procedures to aid in diagnosing file creation problems.

Errors in mm_init

An Error in mm_init error generally indicates an IMTA configuration problem. Thus the `imta-test-rewrite` utility, which is often used to test the health of an IMTA configuration, may return such an error, as may other utilities such as `imta cnbuild`, or a channel, or server, or user agent trying to run may return such an error.

In particular, one of the more commonly encountered sorts of mm_init errors is a “No room in table” error or similar “No room in ...” sort of error. Generally, “no room in” errors are an indication that your current IMTA configuration has not set internal table sizes sufficient for the size of your IMTA configuration, and that it is time to have the IMTA resize its internal tables. (Note that the IMTA stores configuration information in internal tables in memory. To prevent unnecessary use of excessive amounts of virtual memory, these tables are allocated with fixed sizes. The sizes of the tables are controlled by values in the IMTA option file.)

However, some particular such “`no room in ...`” error messages may have alternate causes, and such cases are called out below. Any other “no room in” errors not explicitly mentioned are most likely simply an indication of a need to resize internal tables.

Rather than manually calculating and setting table sizes, you should use the `imta cnbuild` utility to automatically resize the tables for you. See the `imta-cnbuild` man page and *SIMS Reference Manual* for more information.

Following are some of the more commonly encountered `mm_init` errors.

`bad equivalence for alias ...`

The right hand side of an alias file entry is improperly formatted.

`cannot open alias include file...`

A file included into the alias file cannot be opened. This typically indicates a protection problem with a file referenced by the file include operator, <. Note that such included files (like the alias file itself) must be world readable.

`duplicate alias(es) found ...`

Two alias file entries have the same left hand side; you will need to find and eliminate the duplication.

`duplicate host in channel table ...`

In its literal meaning, this error says that you have two channel definitions in the IMTA configuration that both have the same official host name.

But note that an extraneous blank line in the rewrite rules (upper portion) of your IMTA configuration file causes the IMTA to interpret the remainder of the configuration file as channel definitions, and as there are often multiple rewrite rules with the same pattern (left hand side), this then causes the IMTA to think it is seeing channel definitions with non-unique official host names. So check your IMTA configuration both for any channel definitions with duplicate official host names, and for any improper blank lines in the upper (rewrite rules) portion of the file.

`duplicate mapping name found ...`

This error literally means that two mapping tables have the same name, and one of the "duplicates" needs to be removed. However, note that formatting errors in the mapping file may cause the IMTA to interpret something not intended as a mapping table name as a mapping table name; for instance, failure to properly indent a mapping table entry will cause the IMTA to think that the left hand side of the entry is actually a mapping table name. So check your mapping file for general format, as well as checking the mapping table names.

`error initializing ch_ facility: compiled character set version mismatch`

Such an error generally means that you need to recompile and reinstall your compiled character set tables via the command:

```
# imta chbuild
```

See the documentation for `imta chbuild` for additional details.

`error initializing ch_ facility: no room in ...`

Such an error likely means that you need to resize your IMTA character set internal tables and then rebuild the compiled character set tables via the commands

```
# imta chbuild -noimage -maximum -option
# imta chbuild
```

See the man page for `imta-chbuild` for additional details.

`local host alias or proper name too long for system ...`

This error literally means that a local host alias or proper name (the optional right hand side in the second or subsequent names in a channel block) is too long. However, note that certain syntax errors earlier in the IMTA configuration file (an extraneous blank line in the rewrite rules, for instance) may cause the IMTA to interpret something not intended as a channel definition as a channel definition. So besides checking the indicated line of the configuration file, also check above that line for other syntax errors and in particular, if the line on which the IMTA issues this error is intended as a rewrite rule, then be sure to check for extraneous blank lines above it.

`mapping name is too long ...`

This error literally means that a mapping table name is too long and needs to be shortened. However, note that formatting errors in the mapping file may cause the IMTA to interpret something not intended as a mapping table name as a mapping table name; for instance, failure to properly indent a mapping table entry will cause the IMTA to think that the left hand side of the entry is actually a mapping table name. So check your mapping file for general format, as well as checking the mapping table names.

`no equivalence addresses for alias ...`

An entry in the alias file is missing a right hand side (translation value).

`no official host name for channel ...`

This error indicates that a channel definition block is missing the required second line (the official host name line). See the Channel Definition Chapter in the *SIMS Reference Manual* for a discussion of the format of channel definition blocks. In particular, note that a blank line is required before and after each channel definition block, but a blank line must not be present between the channel name and official host name lines of the channel definition; also note that blank lines are not permitted in the rewrite rules portion of the IMTA configuration file.

`no room in ...`

Generally, "`no room in`" errors are an indication that your current IMTA configuration has not set internal table sizes sufficient for the size of your IMTA configuration, and that it is time to have the IMTA resize its internal tables. See the `imta-cnbuild` man page and *SIMS Reference Manual*. However, some particular such "`no room in...`" error messages may have alternate causes, and such cases are called out below. Any other "`no room in...`" errors not explicitly mentioned are most likely simply an indication of a need to resize internal tables.

`no room in channel host table for ...`

This error indicates that your configuration's current IMTA internal table sizes are not large enough for the number of host names listed in your channel definitions. However, note that an extraneous blank line in the rewrite rules (upper portion) of your IMTA configuration file causes the IMTA to interpret the remainder of the configuration file as channel definitions; with just one such extraneous blank line, the IMTA sees just one extra channel but with a lot (all the rest of the rewrite rules) as host names on that channel. So check the line of the file that the error is complaining about---if it is not truly intended as a host name on a channel definition but rather is a line in the rewrite rules section of your configuration file, then check for an extraneous blank line above it.

`no room in channel table for ...`

This error indicates that your configuration's current IMTA internal table sizes are not large enough for the number of channels defined in your IMTA configuration. See `cnbuild` man page and *SIMS Reference Manual*.

`no room in table for alias ...`

This error says that the current IMTA internal table sizes are too small for the number of aliases in the aliases file. This can be resolved either by resizing IMTA's internal table sizes—see the `cnbuild` man page and *SIMS Reference Manual*.

`no room in table for mapping named ...`

In its literal meaning, this error says that your configuration's current IMTA internal table sizes are not large enough for your current number of mapping tables. Internal IMTA table sizes can be increased to match your current configuration side—see the `cnbuild` man page and *SIMS Reference Manual*. However, also note that formatting errors in the IMTA mapping file can cause the IMTA to think that you have more mapping tables than you really have; for instance, check that mapping table entries are all properly indented.

`official host is too long`

The official host name for a channel (second line of the channel definition block) is limited to forty characters in length. So if you were trying to use a longer official host name on a channel, shorten it to a "placeholder" name and then use a rewrite rule to match the longer name to the short official host name. Note, however, that certain syntax errors earlier in the IMTA configuration file (an extraneous blank line in the rewrite rules, for instance) may cause the IMTA to interpret something not intended as a channel definition as a channel definition; that could result in an intended rewrite rule being interpreted as an official host name. So besides checking the indicated line of the configuration file, also check above that line for other syntax errors and in particular, if the line on which the IMTA issues this error is intended as a rewrite rule, then be sure to check for extraneous blank lines above it.

Log File Error Messages

The following error messages would be found in a log file.

`Illegal host/domain errors`

Such an error may be returned immediately in response to an address provided to the IMTA through a user agent, or the error may be deferred and returned as part of an error return mail message. In all cases, such an error message indicates that the IMTA is not able to deliver mail to the specified host. Before diagnosing such problems any further, verify that the address in question is indeed correct and is not misspelled, transcribed incorrectly, or using the name of a host or domain which no longer exists.

Try running the address in question through the `imta test -rewrite` utility. If this utility also returns an "illegal host/domain" error on the address, then the IMTA has no rules in its configuration file, `imta.cnf` and related files, to handle the address. Verify that you have configured the IMTA correctly, that you answered all configuration questions appropriately, and that you have kept your configuration information up to date.

Otherwise, if `imta test -rewrite` does not encounter an error on the address, then the IMTA was able to determine how to handle the address, but the network transport would not accept it. You can examine the appropriate log files from the delivery attempt for additional details. Transient network routing or name service errors should not result in returned error messages, though it is possible for badly misconfigured domain name servers to cause such problems.

If you are on the Internet, then check that MX record lookups work.

`Errors in SMTP channels: os_smtp_* errors`

`os_smtp_* errors`, for example, `os_smtp_open`, `os_smtp_read`, or `os_smtp_write` errors, are not IMTA errors per se: they correspond to the IMTA reporting back about a problem encountered at the network layer. For instance, an os_smtp_open error means that the network connection to the remote side could not be opened, which may be due to addressing errors or channel configuration errors (the IMTA configured to attempt to connect to the “wrong” system), but is more commonly due to DNS problems or network connectivity problems (particularly if this is a channel or address that was previously working). os_smtp_read or os_smtp_write errors are usually an indication that the connection was aborted (either by the other side or due to network problems).

Note that network and DNS problems are often transient in nature. It is normal to occasionally see such problems. Indeed, for connections to troublesome systems, it may even be common. So the occasional such error is usually nothing to be concerned about. However, if you are consistently seeing such errors on most messages on a channel, or seeing such errors on most messages to or from a particular remote system, then the errors may be an indication of an underlying network problem.

If you need more information about an os_smtp_* error, enable debugging on the channel in question and get a debug channel log file showing details of the attempted SMTP dialogue. In particular, the timing of exactly when a network problem occurred during the SMTP dialogue tends to be suggestive as to what sort of network or remote side issue might be involved. In some cases, you may also want to do network level debugging (e.g., TCP/IP packet tracing) to see what was sent or received over the wire.

Queue Monitor Error Messages

This section contains error messages that you may receive while using the Queue Monitor, an explanation of the problem, and instructions on how to resolve the problem, if applicable.

`qmonitorSvr.SelectMtaChannel(qChannel) of QMonitorPanel(): Channel created but yet to be configured.`

The object classes involved may not yet be assigned memory. Close extra windows or applications on your desktop and re-try again.

`getQueMonitorRemoteObj() in QMonitorPanel: QUEUE MONITOR: Could not communicate with the server due to a network problem.`

The IMTA may be down. Check the System Status section on the Admin Console home page to determine the status of the IMTA. If the IMTA is down, start it from the IMTA property book by clicking on the IMTA menu and selecting Start IMTA. If taking this action does not resolve this problem, contact your authorized service provider.

`channelList.addElement in QMonitorPanel: Could not add channels to channel list.`

There may be a network problem or the server may be down. Check your admin server, if it is down, restart the server, and then restart console.

`Init() in QMonitorPanel: Could not allocate memory for resource creation.`

The object classes involved may not yet be assigned memory. Close extra windows or applications on your desktop and re-try again.

`Error getting imageURL of QMonitorPanel:LoadImageURLException`

Any or all pieces of the Uniform Resource Locator (URL) are not in the proper format. Contact your authorized service provider.

`setChoiceBar() of QMonitorPanel: Could not allocate memory for resource creation.`

The object classes involved may not yet be assigned memory. Close extra windows or applications on your desktop and re-try again.

`scaleCounters() of QMonitorPanel: Could not allocate memory for resource creation.`

The object classes involved may not yet be assigned memory. Close extra windows or applications on your desktop and re-try again.

`updateCounterDisplay() of QMonitorPanel: Could not allocate memory for resource creation.`

The object classes involved may not yet be assigned memory. Close extra windows or applications on your desktop and re-try again.

`constructMsgCount() of QMonitorPanel: Could not allocate memory for resource creation.`

The object classes involved may not yet be assigned memory. Close extra windows or applications on your desktop and re-try again.

`constructMsgVolume() of QMonitorPanel: Could not allocate memory for resource creation.`

The object classes involved may not yet be assigned memory. Close extra windows or applications on your desktop and re-try again.

`constructDualGauge() of QMonitorPanel: Could not allocate memory for resource creation.`

The object classes involved may not yet be assigned memory. Close extra windows or applications on your desktop and re-try again.

`Notation() of QMonitorPanel: Could not allocate memory for resource creation.`

The object classes involved may not yet be assigned memory. Close extra windows or applications on your desktop and re-try again.

`getStoredMessages() of handleevent() in QMonitorPanel: QUEUE MONITOR: Could not communicate with the server due to a network problem.`

The IMTA may be down or the Admin server may be down. If the IMTA is down, start it from the IMTA property book by clicking on the IMTA menu and selecting Start IMTA. If the Admin Server is down, restart the server, and then restart console.

`Channel <channel name: No Messages>`

There are no stored messages in the selected channel. Select a channel which has stored messages and try again.

`ResetCounters() of handleevent() in QMonitorPanel: QUEUE MONITOR: Could not communicate with the server due to a network problem.`

The IMTA may be down. Check the System Status section.

`ResetCounters() of handleevent() in QMonitorPanel: Could not allocate memory for resource creation.`

The object classes involved may not yet be assigned memory. Contact your...

`Error in run() of QmonitorPanel Could not allocate memory for resource creation.`

The thread that should be running may have been interrupted by another thread. Contact your authorized service provider.

`Server Polling in run() of QMonitorPanel QUEUE MONITOR: Could not communicate with the server due to a network problem.`

The IMTA may be down. Check the System Status section...

Message Access Protocols Error Messages

`Failed to start IMAP4/POP3.`

The IMAP4/POP3 server cannot start. Contact your authorized service provider.

`Failed to stop IMAP4/POP3.`

The IMAP4/POP3 server cannot stop. Contact your authorized service provider.

`IMAP4/POP3 are already started.`

You are attempting to start the IMAP4/POP3 server when it is already up.

`IMAP4/POP3 are already stopped.`

You are attempting to stop the IMAP4/POP3 server when it has already down.

`You should start IMAP4/POP3 in advance.`

You requested connection information when the IMAP4/POP3 server is not running. Start the IMAP4/POP3 server from the Internet Message Access Protocols property book by clicking on the Internet Message Access Protocols menu and selecting start message access protocols IMAP4/POP3.

Message Store Error Messages

Error messages and warnings concerning the message store and the programs which maintain it, such as the mail server and mail delivery, often will report to the system log, `/var/log/syslog`.

Besides normally checking syslog periodically, if any unexpected effects are noticed, the admin should check the syslog for messages concerning the message store.

For example, if you can not connect to the mail server through IMAP after a system crash, check the syslog to see if the mail server (imaccessd) has exited and left a message as to why. It is possible the mail server may explain that the store is in a questionable state, and imcheck must be run for crash recovery before the store will be allowed back up.

Even if the store comes up, it is possible that warning or error messages may be sent during delivery or access to syslog in unexpected situations. Usually these messages specify a user or day that has some kind of problem which may or may not need to be addressed. Often with the user or day information, an admin can run imcheck on that user or day in order to get more information and to see if there is a problem.

Glossary

ACAP Application Configuration Access Protocol. A protocol which enhances IMAP by allowing the user to set up address books, user options, and other data for universal access.

access control rules Rules specifying user permissions for a given set of directory entries or attributes.

access control list (ACL) A set of data associated with a directory that defines the permissions that users and/or groups have for accessing it.

Administration Console or Admin Console A GUI (graphical user interface) which enables you to configure, monitor, maintain, and troubleshoot the SIMS components.

address mapping See forward address mapping or reverse address mapping.

address token The address element of a rewrite rule pattern.

Administration Services A service daemon that administers components of SIMS through a GUI.

agent In the client-server model, the part of the system that performs information preparation and exchange on behalf of a client or server application. See also *MTA*.

alias An alternate name of an email address.

alias file A file used to set aliases not set in a directory, such as the postmaster alias.

APOP Authenticated Post Office Protocol. Similar to the Post Office Protocol (POP), but instead of using a plaintext password for authentication, it uses an encoding of the password together with a challenge string.

attribute The form of information stored and retrieved by the directory service. Directory information consists of entries, each containing one or more attributes. Each attribute consists of a type identifier together with one or more values. Each directory read operation can retrieve some or all attributes from a designated entry.

attribute index An index, or list, of entries which contains a given attribute or attribute value.

autoreply option file A file used for setting options for autoreply, such as vacation notices.

backbone The primary connectivity mechanism of a distributed system. All systems that have connectivity to an intermediate system on the backbone are connected to each other. This does not prevent you from setting up systems to bypass the backbone for reasons of cost, performance, or security.

bang path An address for sending e-mail via UUCP that specifies the entire route to the destination computer. It separates each host name with an exclamation point, which is also known as a bang. For example, the bang path `midearth!shire!bilbo!jsmith` would go to the `jsmith` user account on the `bilbo` host, which is reached by first going to `midearth` and then `shire`.

CA Certificate Authority. An organization that issues digital certificates (digital identification) and makes its public key widely available to its intended audience.

directory cache A temporary storage of information that has been retrieved from the directory.

Certificate Authority See CA.

channel An interface with another SIMS component, another email system, or a mail user agent.

character set labels A name or label for a character set.

client-server model A computing model in which powerful networked computers provide specific services to other client computers. Examples include the name-server/name-resolver paradigm of the DNS and fileserver/file-client relationships such as NFS and diskless hosts.

cn LDAP alias for common name.

composition The process of constructing a message by the Mail User Agent (MUA). See also *MUA*.

configuration file A file that contains the configuration parameters for a specific component of the SIMS system.

congestion thresholds A disk space limit that can be set by the system administrator that prevents the database from becoming overloaded by restricting new operations when system resources are insufficient.

conversion channel Converts body of messages from one form to another.

cookie Cookies are text-only strings entered into the browser’s memory automatically when you visit specific web sites. Cookies are programmed by the web page author. Users can either accept or deny cookies. Accepting the cookies allows the web page to load more quickly and is not a threat to the security of your machine.

ciphertext Text which has been encrypted. Opposite of plaintext.

daemon A UNIX program that is not invoked explicitly, but lies dormant waiting for some condition(s) to occur. The instigator of the condition need not be aware that a daemon is lurking (though often a program will commit an action only because it knows that it will implicitly invoke a daemon). Typical daemons are print spoolers, e-mail handlers, and schedulers that start up another process at a designated time or condition.

data store A store that contains directory information, typically for an entire directory information tree.

DC tree Domain Component tree. A directory information tree that mirrors the DNS network syntax. An example of a distinguished name in an DC tree would be `cn=billbob,dc=bridge,dc=net,o=internet`

defragmentation The Multiple Internet Mail Extensions (MIME) feature that enables a large message that has been broken down into smaller messages or fragments to be reassembled. A Message Partial Content-Type header field that appears in each of the fragments contains information that helps reassemble the fragments into one message. See also *fragmentation*.

delegated administrator A person who has the privileges to add, modify, delete, and search for group or user entries at a specified hosted domain.

Delegated Management Console A web browser-based software console that allows delegated administrators to add and modify users and groups to a hosted domain. Also allows end users to change their password, set message forwarding rules, set vacation rules, and list distribution list subscriptions.

delegated management server A daemon program that handles access control to the directory by hosted domains.

denial of service attack A situation where an individual intentionally or inadvertently overwhelms your mail server by flooding it with messages. Your server's throughput could be significantly impacted or the server itself could become overloaded and nonfunctional.

dereferencing an alias Specifying, in a bind or search operation, that a directory service translate an alias distinguished name to the actual distinguished name of an entry.

destination channel The last element of a host/domain rewrite rule, in whose queue a message should be placed in for delivery.

directory cache A cache containing the directory information used by the IMTA to deliver mail.

directory context The point in the directory tree information at which a search begins for entries used to authenticate a user and password for Sun Message Store access.

directory entry A set of directory attributes and their values identified by its distinguished name. Each entry contains an object class attribute that specifies the kind of object the entry describes and defines the set of attributes it contains. Also called the *IMTA directory cache.*

directory information tree The tree-like hierarchical structure in which directory entries are organized. Also called a DIT. DITs can be organized along the DNS (DC trees) or Open Systems Interconnect networks (OSI trees).

directory schema The set of rules that defines the data that can be stored in the directory.

directory service A logically centralized repository of information. The component in SIMS that stores user, distribution list, and configuration data.

directory synchronization Because information stored in the directory service is updated as new entries are added, modified and deleted, the information in the IMTA directory cache must be periodically updated with the current information in the directory service. This process is called directory synchronization. Sometimes called a dirsync in reference to the `imta dirsync` command.

dirsync option file A file used to set options for the `dirsync` program which cannot be set through the command line.

disconnected state The mail client connects to the server, makes a cache copy of selected messages, then disconnects from the server.

distinguished name The comma-separated sequence of attributes and values that specify the unique location of an entry within the directory information tree. Often abbreviated as DN.

distribution list A list of email addresses (users) that can be sent a message by specifying one email address. Also called a group. See also *expansion, member, moderator, owner,* and *alias*.

distribution list owner An individual who is responsible for a distribution list. An owner can add or delete distribution list members. See also *distribution list*, *expansion*, *member*, and *moderator.*

DIT See *directory information tree.*

DN Distinguished name.

dn LDAP alias for distinguished name.

DNS Domain Name System. A distributed name resolution software that allows computers to locate other computers on a UNIX network or the Internet by domain name. DNS servers provide a distributed, replicated, data query service for translating hostnames into Internet addresses.

DNS database A database of domain names (host names) and their corresponding IP addresses.

domain A group of computers whose hostnames share a common suffix, the *domain name*. Syntactically, an Internet domain name consists of a sequence of names (labels) separated by periods (dots), for example, `tundra.mpk.ca.us`.

domain quota The amount of space, configured by the system administrator, allocated to a domain for email messages.

domain rewriting rules See also *rewrite rules*.

domain template The part of a rewrite rule that defines how the host/domain portion of an address is rewritten. It can include either a full static host/domain address or a single field substitution string, or both.

dsservd A daemon that operates that accesses the database files that hold the directory information, and communicates with directory clients using the LDAP protocol.

EMAPI Extended MAPI Service Provider. Transparently turns Microsoft Exchange client into an Internet standard IMAP/LDAP client. See also *IMAP*, *LDAP*.

encryption Scrambling the contents of a message so that its contents cannot be read without the encryption, or code key.

entries User, group, or organizational data used to configure message accounts.

envelope The part of an Internet mail message that contains the delivery information. The envelope contains the originator and recipient information associated with a message.

ESMTP Extended Simple Mail Transfer Protocol. An Internet message transport protocol.

expander Part of an electronic mail delivery system which allows a message to be delivered to a list of addressees. Mail expanders are used to implement mailing lists. Users send messages to a single address (e.g., hacks@somehost.edu) and the mail expander takes care of delivery to the mailboxes in the list. Also called *mail exploders*.

expansion This term applies to the IMTA processing of distribution lists. The act of converting a message addressed to a distribution list into enough copies for each distribution list member.

expunge The act of marking a message for deletion and then permanently removing it from you INBOX.

external channel An interface between the IMTA and either another SIMS component or another component outside the SIMS email system.

failover The automatic transfer of a computer service from one system to another to provide redundant backup.

Filesharing Transport This type of transport moves messages between the UNIX operating system and the PC running a client through a shared file system available to both platforms. When a channel is configured to use filesharing transport, the shared directory to use for the file exchange must be specified.

firewall A dedicated gateway machine with special security precautions used to service outside network, especially Internet, connections and dial-in lines. The idea is to protect a cluster of more loosely administered machines hidden behind the firewall from unwanted entry from outside the firewall.

folder Named place where mail is stored. Also called a *mailbox*. Inbox is a folder that stores new mail. Users can also have folders where mail can be stored. A folder can contain other folders in a hierarchical tree. Folders owned by a user are called *private folders*. See also *shared folders*.

Folder Check A utility which checks the accessibility of messages and folders and verifies links. This utility is used as part of the regular maintenance of SIMS.

forward address mapping Message envelopes, TO:address, are processed to a mapping table. The result of the mapping is tested. If necessary, the exact form of the envelope is exchanged for another which can then be processed by a different, and perhaps non-compliant RFC 822, mail system.

FQDN See fully qualified domain name.

fragmentation The Multiple Internet Mail Extensions (MIME) feature that allows the breaking up of a large message into smaller messages. See also *defragmentation*.

full static host/domain address The portion of a host/domain address elements set off by decimals as part of the domain template. See also *domain template*.

fully qualified domain name The full name of a system, consisting of its local host name and its domain name. For example, *class* is a host name and *class.sun.edu* is an fully qualified domain name. A fully qualified domain name should be sufficient to determine a unique Internet address for any host on the Internet. The same naming scheme is also used for some hosts that are not on the Internet, but share the same name-space for electronic mail addressing. A host which does not have a fully qualified domain name must be addressed using a bang path.

gateway The terms *gateway* and *application gateway* refer to systems that do translation from one native format to another. Examples include X.400 to/from RFC 822 electronic mail gateways. A machine that connects two or more electronic mail systems (especially dissimilar mail systems on two different networks) and transfers messages between them. Sometimes the mapping and translation can be complex, and it generally requires a store-and-forward scheme whereby the message is received from one system completely before it is transmitted to the next system after suitable translations.

global log manager A utility that handles log information from each Sun Internet Mail Server component.

group Same as a distribution list.

group folders These contain folders for shared and group folders. See *shared folder.*

header The part of an Internet mail message that is composed of a field name followed by a colon and then a value. Headers include delivery information, summaries of contents, tracing, and MIME information.

hosted domain An email domain that is outsourced by an ISP. That is, the ISP provides email domain hosting for an organization by operating and maintaining the email services for that organization. A hosted domain shares the same SIMS host with other hosted domains. In earlier LDAP-based email systems, a domain was supported one or more email server hosts. With SIMS, many domains can be hosted on a single server. Hosted domains are also called *virtual hosted domains* or *virtual domains*.

host name The logical name assigned to a computer. On the Web, most hosts are named `www`; for example, `www.mycompany.com`. If a site is composed of several hosts, they might be given different names such as `support.mycompany.com` and `sales.mycompany.com`. `support` and `sales` are the host names, `mycompany` is the subdomain name, and `com` is the top-level domain name.

IMAP4 Internet Message Access Protocol. IMAP4 provides advanced disconnected mode client access.

IMTA Internet Message Transfer Agent. IMTA routes, transports, and delivers Internet Mail messages within the email system.

internal channel An interface between internal modules of the IMTA. Internal channels include the reprocessing, conversion, and defragmentation channels. These channels are not configurable.

Internet A collection of networks interconnected by a set of routers that allow them to function as the largest single world-wide virtual network.

internet protocol address A 32-bit address assigned to hosts using TCP/IP. Also called the *IP address* and *internet address.*

invalid user An error condition that occurs during message handling. When this occurs, the message store sends a communication to the Internet Message Transport Agent (IMTA), the message store deletes its copy of the message. The IMTA bounces the message back to the sender and deletes its copy of the message.

ISP Internet Service Provider. A company that provides internet services to its customers including email, electronic calendaring, access to the world wide web, and web hosting.

job controller An IMTA daemon responsible for scheduling message delivery. Job controller also controls channel queues and determines the order of processing. Requests are processed in the order in which they are received by the system.

knowledge information Part of the directory service infrastructure information. The directory server uses knowledge information to pass requests for information to other servers.

LDAP Lightweight Directory Access Protocol. LDAP is a protocol used for the storage, retrieval, and distribution of information, including user profiles, distribution lists, and configuration data.

LDAP referrals An LDAP entry that consists of a symbolic link (referral) to another LDAP entry. An LDAP referral consists of an LDAP host and a distinguished name. LDAP referrals are often used to reference existing LDAP data so that this data does not have to be replicated. They are also used to maintain compatibility for programs that depend on a particular entry that may have been moved.

LDAP Server A software server that maintains an LDAP directory and services queries to the directory. The Sun Directory Services and the Netscape Directory Services are implementations of an LDAP Server.

LDAP server failover A backup feature for LDAP servers. If one LDAP server fails, the system can switch over to another LDAP server.

LDAP filter A way of specifying a set of entries, based on the presence of a particular attribute or attribute value.

LDBM LDAP Data Base Manager.

LDIF LDAP Data Interchange Format. A data format used to represent LDAP entries in text form.

local channel A channel that allows you to determine delivery options of local users and delivers mail to Solaris Operating Environment mailboxes.

lookup Same as a search, using the specified parameters for sorting data.

mailbox A place where messages are stored and viewed. See *folder*.

managed object A collection of configurable attributes, for example, a collection of attributes for the directory service.

mapping tables Two column tables which transform, map, an input string into an output string.

master directory server The directory server that contains the data that will be replicated.

master message catalog Contains message catalogs for the SIMS components.

master program A channel program that initiates a message transfer to another interface on its own.

member A user or group who receives a copy of an email addressed to a distribution list. See also *distribution list*, *expansion*, *moderator*, and *owner*.

Message Access and Store The SIMS components which store user messages and allow for retrieval and processing of messages.

Message Access Services Consists of protocol servers, software drivers, and libraries which support client access to the message store.

message access services The drivers and libraries that support client access to the SIMS message store.

message catalogs The log messages, command line responses, and graphical user interface screen text contained in the SIMS components.

message submission The client Mail User Agent (MUA) transfers a message to the mail server and requests delivery.

MIB Management Information Base. A collection of objects that can be accessed via a network management protocol. See also *SMI*.

MIME Multipurpose Internet Mail Extensions. A format for defining email message content.

moderator A person who first receives all email addressed to a distribution list before A) forwarding the message to the distribution list, B) editing the message and then forwarding it to the distribution list, or C) not forwarding the message to the distribution list. See also *distribution list*, *expansion*, *member*, and *owner*.

MTA Message Transfer Agent. An OSI application process used to store and forward messages in the X.400 Message Handling System. Equivalent to Internet mail agent. See *IMTA*.

MUA Mail User Agent. The client applications invoked by end users to read, submit, and organize their electronic mail.

mx record Mail Exchange Record. A DNS resource record stating a host that can handle electronic mail for a particular domain.

name resolution The process of mapping an IP address to the corresponding name. See also *DNS*.

namespace The space from which an object name is derived and understood. Files are named within the file namespace, domain components are named within the domain namespace.

naming attribute The final attribute in a directory information tree distinguished name. See also *relative distinguished name.*

naming context A specific subtree of a directory information tree that is identified by its DN. In SIMS, specific types of directory information are stored in naming contexts. For example, a naming context which stores all entries for marketing employees in the XYZ Corporation at the Boston office might be called ou=mktg, ou=Boston, o=XYZ, c=US.

NIS A distributed network information service containing key information about the systems and the users on the network. The NIS database is stored on the master server and all the replica or slave servers.

NIS+ A distributed network information service containing hierarchical information about the systems and the users on the network. The NIS+ database is stored on the master server and all the replica servers.

nondelivery report During message transmission, if the IMTA does not find a match between the address pattern and a rewrite rule, the IMTA sends a nondelivery report back to the sender with the original message.

notary messages Text messages sent by the MTA to an email sender indicating delivery or non-delivery status of a sent message.

o LDAP alias for `organization`

object class A template specifying the kind of object the entry describes and the set of attributes it contains. For example, SIMS specifies an `emailPerson` object class which has attributes such as `commonname`, `mail` (email address), `mailHost`, and `mailQuota`.

off-line state The mail client fetches messages from a server system to a client system, which may be a desktop or portable system and may delete them from the server. The mail client downloads the messages where they can be viewed and answered.

on-line state A state in which messages remain on the server and are remotely responded to by the mail client.

option files IMTA option files contain global parameters used to override default values of parameters which apply to IMTA as a whole, such as sizes for various tables into which various configuration and alias files are read.

OSI tree A directory information tree that mirrors the Open Systems Interconnect network syntax. An example of a distinguished name in an OSI tree would be `cn=billt,o=bridge,c=us`

ou LDAP alias for `organizationalUnit`

permanent failure An error condition that occurs during message handling. When this occurs, the message store deletes its copy of an email message. The Internet Message Transport Agent (IMTA) bounces the message back to the sender and deletes its copy of the message.

pipe channel A channel which performs delivery of messages via a per-user-site-supplied program. These programs must be registered in SIMS by the system administrator, and thus do not pose a security risk.

plaintext Unencrypted readable text. The opposite of cypher text

plaintext authentication Authentication that occurs by sending passwords over the network in plaintext. Considered a security problem since plaintext passwords can be easily captured over a network.

POP Post Office Protocol. POP provides remote access support for older mail clients.

populating the directory Entering information for users and distribution lists to the SIMS directory service.

protocol A formal description of messages to be exchanged and rules to be followed for two or more systems to exchange information.

provisioning The process of adding, modifying or deleting entries in the SIMS directory service. These entries include users and groups.

provisioning commands SIMS commands that provide provisioning functions. These commands are prefaced with `imadmin`.

proxy The mechanism whereby one system “fronts for” another system in responding to protocol requests. Proxy systems are used in network management to avoid having to implement full protocol stacks in simple devices, such as modems.

public key encryption A cryptographic method that uses a two-part key (code) that is made up of public and private components. To encrypt messages, the published public keys of the recipients are used. To decrypt the messages, the recipients use their unpublished private keys known only to them.

purge The process of permanently removing messages that have been deleted and are no longer referenced in user and group folders and returning the space to the Sun Message Store file system. See also *backup* and *restore*.

quota See user quota.

referral A process by which the directory server returns an information request to the client that submitted it, with information about the Directory Service Agent (DSA) that the client should contact with the request. See also *knowledge information*.

relaying A message is passed from one mail server to another mail server.

relative distinguished name The final attribute and its value in the attribute and value sequence of the distinguished name. See also *distinguished name*.

replica directory server The directory that will receive a copy of all or part of the data.

reprocessing channel Performs deferred processing. The reprocessing channel is the intersection of all other channel programs. It performs only the operations that are shared with other channels.

restore The process of restoring the contents of folders from a backup device to the Sun Message Store. See also *backup* and *purge*.

reverse address mapping Addresses are processed to a mapping table, with a reversal database, generally substituting a generic address, possibly on a central machine, for an address on a remote or transitory system.

rewrite rules Also known as domain rewriting rules. A tool that the Internet Mail Transport Agent (IMTA) uses to route messages to the correct host for delivery. Rewrite rules perform the following functions: (1) extract the host/domain specification from an address of an incoming message, (2) match the host/domain specification with a rewrite rule pattern, (3) rewrite the host/domain specification based on the domain template, and (4) decide which IMTA channel queue the message should be placed in.

RFC Request For Comments. The document series, begun in 1969, describes the Internet suite of protocols and related experiments. Not all (in fact very few) RFCs describe Internet standards, but all Internet standards are published as RFCs. See `http://www.imc.org/rfcs.html`.

root entry The first entry of the directory information tree (DIT) hierarchy.

router A system responsible for determining which of several paths network traffic will follow. It uses a routing protocol to gain information about the network, and algorithms to choose the best route based on several criteria known as “routing metrics.” In OSI terminology, a router is a Network Layer intermediate system. See also *gateway*.

routability scope Specifications which enable the IMTA to send messages by the most direct route, either to a specific user's folder, a group of folders, or to a mail host.

routing In an email system, the act of delivering a message based on addressing information extracted from the body of the message. The Internet Message Transfer Agent (IMTA) is the component responsible for routing messages.

safe file system A file system performs logging such that if a system crashes it is possible to rollback the data to a pre-crash state and restore all data. An example of a safe file system is Veritas File System, VxFS.

schema A set of rules which sets the parameters of the data stored in a directory. It defines the type of entries, their structure and their syntax.

sendmail This program acts as a mail transport agent for Solaris software. It is responsible for routing mail and resolution of mail addresses.

shared folder or shared mailbox *A* mailbox that can be viewed by members of a *distribution list*. Shared folders have an *owner* who can add or delete members to the group and can delete messages from a the shared folder. The can also have a moderator who can edit, block, or forward incoming messages.

SIMS administrator An individual who has a valid log in and password for the SIMS Admin Console. This person can also use this log in and password to execute the provisioning CLIs.

single field substitution string Part of the domain template that dynamically rewrites the specified address token of the host/domain address. See also *domain template*.

SKIP Simple Key management for IP. A security system that encrypts or scrambles the text of a message so only the receiving mail client or message server can decrypt or unscramble the text.

slave program A channel program that accepts transfers initiated by another interface.

smart host The mail server in a domain to which other mail servers, forward messages if they do not recognize the recipients.

SMTP Simple Mail Transfer Protocol. The Internet electronic mail protocol. Defined in RFC 821, with associated message format descriptions in RFC 822.

SMTP Dispatcher A multithreaded connection dispatching agent which allows multiple multithreaded servers to share responsibility for a given service, thus allowing several multithreaded SMTP servers to run concurrently and handle one or more active connections.

SMTP intranet or internet channel A channel dedicated to relaying messages between the IMTA and a group of SMTP hosts within, or outside of, your mail network.

SMTP router channel SMTP channel that handles messages between the IMTA and firewall host.

sn LDAP alias for `surname`

SNMP Simple Network Management Protocol. The network management protocol of choice for TCP/IP-based internets.

subordinate reference The naming context that is a child of the naming context held by your directory server. See also *knowledge information*.

Sun Directory Services Sun Microsystems' implementation of an LDAP directory server. Provides storage of, and access to, user profiles, distribution lists, and other SIMS information. The Sun Directory Services is one of the three main SIMS components along with the IMTA and MS/MA.

Sun Internet Mail Server An enterprise-wide, open-standards based, scalable electronic message-handling system.

Sun Message Store The server from which mail clients retrieve and submit messages.

SSL Secure Sockets Layer is an open, non-proprietary security protocol for authenticated and encrypted communication between clients and servers.

synchronization The update of data by a master directory server to a replica directory server.

table lookup With a table consisting of two columns of data, an input string is compared with the data within the table and transformed to an output string.

tailor file An option file used to set the location of various IMTA components.

transient failure An error condition that occurs during message handling. The remote Internet Message Transport Agent (IMTA) is unable to handle the message when it's delivered, but may be able to later. The local IMTA returns the message to the channel queue and schedules it for retransmission at a later time.

transport protocols Provides the means to transfer messages between message stores.

uid User identification. A unique string identifying a user to a system. Also referred to as a userid.

unsafe file system A file system that does not perform logging. If the system crashes, the state cannot be recreated and some data may be lost. You must also perform `imcheck` before activating message access to these files.

upper reference Indicates the directory server that holds the naming context above your directory server's naming context in the directory information tree (DIT).

user entry or user profile Fields that describe information about each user, required and optional, examples are: distinguished name, full name, title, telephone number, pager number, login name, password, home directory, etc.

user folders A user's email mailboxes.

user quota The amount of space, configured by the system administrator, allocated to a user for email messages.

user redirection The remote Internet Message Transport Agent (IMTA) cannot accept mail for the recipient, but can reroute the mail to a mail server that can accept it.

UUCP UNIX to UNIX Copy Program. A protocol used for communication between consenting UNIX systems.

valid user A condition that occurs during message handling. After the message store sends a communication to the Internet Message Transport Agent (IMTA), the IMTA deletes its copy of the message and it is now the message store's responsibility.

`/var/mail` The UNIX version 7 “`From`” delimited mailbox as implemented in the Solaris operating system.

virtual hosted domains or virtual domains See *hosted domains*.

workgroup Local workgroup environment, where the server performs its own routing and delivery within a local office or workgroup. Interdepartmental mail is routed to a backbone server. See also *backbone*.

X.400 A message handling system standard.

Index